09/504070

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年 ９月 １日

出 願 番 号
Application Number: 平成１１年特許願第２４７４５７号

出 願 人
Applicant (s): 日本電信電話株式会社

CERTIFIED COPY OF PRIORITY DOCUMENT

２０００年 １月１４日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆 彦

【書類名】　特許願

【整理番号】　NTTH115883

【提出日】　平成11年 9月 1日

【あて先】　特許庁長官　伊佐山　建志　殿

【国際特許分類】　G06F 15/21

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　寺田　雅之

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　藤村　考

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　久野　浩

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　花館　蔵之

【特許出願人】

【識別番号】　000004226

【氏名又は名称】　日本電信電話株式会社

【代理人】

【識別番号】　100070150

【弁理士】

【氏名又は名称】　伊東　忠彦

【手数料の表示】

【予納台帳番号】　002989

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　原本データ流通システム及び原本データ流通プログラムを格納した記憶媒体

【特許請求の範囲】

【請求項１】　電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、

ある装置に対応する第１の情報と、データもしくは、データに対応する情報である第２の情報と、から構成される原本性情報を転送する転送手段を有する第１の装置と、

前記原本性情報の転送元装置を特定する特定手段と、該転送元装置が認証された場合に該原本性情報を有効であると判別する第１の認証手段と、該転送元装置と該原本性情報の第１の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判別する第２の認証手段とを有する第２の装置とを有することを特徴とする原本データ流通システム。

【請求項２】　前記第１の装置は、

秘密鍵を秘匿する手段を更に有し、

前記第２の装置は、

１乃至、複数の秘密鍵に対応する公開鍵の一方向関数による出力である自装置のフィンガープリントを保持、または、入手する手段を更に有し、

前記第２の装置の前記第１の認証手段は、

転送元の前記第１の装置が前記フィンガープリントに対応する秘密鍵を保持していることを検証することにより、該転送元の第１の装置を認証する請求項１記載の原本データ流通システム。

【請求項３】　前記第１の装置の前記転送手段は、

自装置が１乃至複数の第三者によって認証されていることを証明する情報であり、該第三者である認証者に対応する情報である第三者証明を前記第２の装置に転送する手段を有し、

前記第２の装置は、

１乃至複数の第三者に対応する第三者情報を保持、または、入手する手段を有

し、

前記第１の認証手段は、

転送元装置である前記第１の装置が前記第三者証明における認証対象であり、かつ、該第三者証明の認証者のいずれかが、保持されている前記第三者情報に対応する第三者に含まれることを検証することにより、該転送元の前記第１の装置を認証する請求項１記載の原本データ流通システム。

【請求項４】　前記第２の装置は、

前記第１の情報と、１乃至複数の第三者に対応する情報とを対応付ける第三者信任情報を保持もしくは、入手する手段を有し、

前記第１の認証手段は、

原本性情報の転送元である前記第１の装置が該第三者証明における認証対象であり、かつ、転送された前記原本性情報の第１の情報から、保持されている前記第三者信任情報を用いて該第１の情報に対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信任情報から抽出された第三者に含まれることを検証することにより、該転送元の第１の装置を認証する請求項３記載の原本データ流通システム。

【請求項５】　前記第２の装置は、

前記第１の情報と前記第２の情報とから、第三者に対応する情報とを対応づける、前記第三者信任情報を保持もしくは、入手する手段を有し、

前記第１の認証手段は、

転送された前記原本性情報の前記第１の情報と前記第２の情報から、前記第三者信任情報を用いて該第１の情報と該第２の情報の対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信任情報から抽出された第三者に含まれることを検証することにより、該転送元の第１の装置を認証する請求項３記載の原本データ流通システム。

【請求項６】　前記第１の装置は、

秘密鍵を秘匿する手段と、

前記秘密鍵に対応した公開鍵に、自装置を認証する第三者が署名を付与した公開鍵証明書と該秘密鍵による署名を前記第２の装置に転送する手段を有し、

前記第２の装置は、

前記公開鍵証明書を検証して署名者の公開鍵を特定する手段と、

１乃至複数のフィガープリントを保持または、入手する手段とを更に有し、

前記第１の認証手段は、

前記秘密鍵による署名を前記公開鍵証明書が含む公開鍵により検証し、かつ、該公開鍵証明書の署名者の公開鍵の一方向関数による出力が、保持されている前記フィンガープリントに含まれることを検証することにより、転送元の前記第１の装置を認証する請求項１記載の原本データ流通システム。

【請求項７】　前記第２の装置は、

前記第１の情報と、１乃至複数の第１の装置に対応する情報とを対応付ける利用者信任情報を保持もしくは、入手する手段を有し、

前記第１の認証手段は、

転送された前記原本性情報の第１の情報から、保持されている前記利用者信任情報を用いて、該第１の情報に対応する第１の装置に対応する情報を抽出し、転送元装置が該利用者信任情報から抽出された第１の装置に含まれることを検証することにより、該転送元の第１の装置を認証する請求項１記載の原本データ流通システム。

【請求項８】　前記第２の装置は、

前記第１の情報と前記第２の情報から、１乃至複数の前記第１の装置に対応する情報を対応付ける利用者信任情報を保持もしくは、入手する手段を有し、

前記第１の認証手段は、

転送された前記原本性情報の第１の情報と第２の情報とから、保持されている前記利用者信任情報を用いて、該第１の情報と該第２の情報に対応する第１の装置に対応する情報を抽出し、転送元装置が、該利用者信任情報から抽出された第１の装置に含まれることを検証することにより、該転送元の第１の装置を認証する請求項１記載の原本データ流通システム。

【請求項９】　電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、

自装置に対応する情報を第１の情報とし、あるデータもしくは、該データに対

応する情報を第２の情報として、原本性情報を生成する原本性情報生成手段と、

前記原本性情報を転送する原本性情報転送手段とを有する発行者装置を有することを特徴とする原本データ流通システム。

【請求項１０】　前記発行者装置は、

秘密鍵を秘匿する手段と、

前記秘密鍵に対応する公開鍵の一方向関数による出力である自装置のフィンガープリントを前記第１の情報として生成する手段を有する請求項９記載の原本データ流通システム。

【請求項１１】　前記発行者装置は、

前記原本性情報の前記第２の情報として、データの一方向関数による出力を生成する手段を有する請求項９記載の原本データ流通システム。

【請求項１２】　前記発行者装置は、

前記原本性情報の前記第２の情報として、ネットワーク上の資源の識別子を用いる請求項１１記載の原本データ流通システム。

【請求項１３】　電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、

ある装置に対応する第１の情報と、データもしくは、データに対応する情報である第２の情報から構成される原本性情報を転送する原本性情報転送手段と、

他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する特定手段と、

前記転送元装置が認証された場合、もしくは、該転送元装置と前記原本性情報の第１の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する認証手段と、

前記認証手段で前記原本性情報が有効であると判別された場合に、該原本性情報を格納する格納手段とを有する利用者装置を有することを特徴とする原本データ流通システム。

【請求項１４】　前記利用者装置は、

自装置から前記原本性情報を転送する際に、該原本性情報を消去する手段を有する請求項１３記載の原本データ流通システム。

【請求項１５】　電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、

原本性情報の転送元装置を特定する特定手段と、

前記転送元装置を認証する認証手段と、

前記認証手段において、自装置に転送された前記原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第２の情報に対応するデータに対応する処理を行うデータ処理手段を有する改札者装置を有することを特徴とする原本データ流通システム。

【請求項１６】　前記改札者装置は、

発行者装置に対応する情報である発行者情報を保持もしくは、入手する手段を更に有し、

前記データ処理手段は、

前記認証手段において、転送された前記原本性情報が有効であると判別され、かつ、該原本性情報の装置に対応する第１の情報に対応する発行者装置が、保持されている前記発行者情報に対応する発行者装置に含まれる場合に、該原本性情報のデータまたは、データに対応する情報である第２の情報に対応するデータに対する処理を行う請求項１５記載の原本データ流通システム。

【請求項１７】　電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、

自装置に対応する情報を第１の情報とし、あるデータもしくは、該データに対応する情報を第２の情報として、原本性情報を生成する第１の原本性情報生成手段と、該原本性情報を転送する第１の原本性情報転送手段とを有する発行者装置と、

ある装置に対応する第１の情報と、データもしくは、データに対応する情報である第２の情報から構成される原本性情報を転送する第２の原本性情報転送手段と、他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する第１の特定手段と、該転送元装置が認証された場合、もしくは、該転送元装置と該原本性情報の第１の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する第１の認証手段と、該第１の認証手段で該原

本性情報が有効であると判別された場合に、該原本性情報を格納する格納手段とを有する利用者装置と、

原本性情報の転送元装置を特定する第２の特定手段と、前記転送元装置を認証する第２の認証手段と、該第２の認証手段において、自装置に転送された該原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第２の情報に対応するデータに対する処理を行うデータ処理手段を有する改札者装置とを有することを特徴とする原本データ流通システム。

【請求項１８】　電子的な情報である原本データの蓄積や流通を行う原本データ流通プログラムを格納した記憶媒体であって、

第１の装置に搭載される、

ある装置に対応する第１の情報と、データもしくは、データに対応する情報である第２の情報と、から構成される原本性情報を転送させる転送プロセスと、

第２の装置に搭載される、

前記原本性情報の転送元装置を特定する特定プロセスと、該転送元装置が認証された場合に該原本性情報を有効であると判別する第１の認証プロセスと、該転送元装置と該原本性情報の第１の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判別する第２の認証プロセスとを有することを特徴とする原本データ流通プログラムを格納した記憶媒体。

【請求項１９】　前記第１の装置に搭載される、秘密鍵を秘匿するプロセスを更に有し、

前記第２の装置に搭載される、

１乃至、複数の秘密鍵に対応する公開鍵の一方向性関数による出力である自装置のフィンガープリントを保持、または、入手するプロセスを更に有し、

前記第１の認証プロセスは、

転送元の前記第１の装置が前記フィンガープリントに対応する秘密鍵を保持していることを検証することにより、該転送元の第１の装置を認証するプロセスを含む請求項１８記載の原本データ流通プログラムを格納した記憶媒体。

【請求項２０】　前記第１の装置に搭載されるの前記転送プロセスは、

自装置が１乃至複数の第三者によって認証されていることを証明する情報であ

り、該第三者である認証者に対応する情報である第三者証明を前記第２の装置に転送するプロセスを有し、

前記第２の装置に搭載される、

１乃至複数の第三者に対応する第三者情報を保持、または、入手するプロセスを有し、

前記第２の装置に搭載される前記第１の認証プロセスは、

転送元装置である前記第１の装置が前記第三者証明における認証対象であり、かつ、該第三者証明の認証者のいずれかが、保持されている前記第三者情報に対応する第三者に含まれることを検証することにより、該転送元の前記第１の装置を認証するプロセスを含む請求項１８記載の原本データ流通プログラムを格納した記憶媒体。

【請求項２１】　前記第２の装置に搭載される、

前記第１の情報と、１乃至複数の第三者に対応する情報とを対応付ける第三者信任情報を保持もしくは、入手するプロセスを有し、

前記第１の認証プロセスは、

原本性情報の転送元である前記第１の装置が該第三者証明における認証対象であり、かつ、転送された前記原本性情報の第１の情報から、保持されている前記第三者信任情報を用いて該第１の情報に対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信任情報から抽出された第三者に含まれることを検証することにより、該転送元の第１の装置を認証するプロセスを含む請求項２０記載の原本データ流通プログラムを格納した記憶媒体。

【請求項２２】　前記第２の装置に搭載される、

前記第１の情報と前記第２の情報とから、第三者に対応する情報とを対応づける、前記第三者信任情報を保持もしくは、入手するプロセスを有し、

前記第１の認証プロセスは、

転送された前記原本性情報の前記第１の情報と前記第２の情報から、前記第三者信任情報を用いて該第１の情報と該第２の情報の対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信任情報から抽出された第三者に含まれることを検証することにより、該転送元の第１の装置を認証

するプロセスを含む請求項２０記載の原本データ流通プログラムを格納した記憶媒体。

【請求項２３】　前記第１の装置に搭載される、

秘密鍵を秘匿するプロセスと、

前記秘密鍵に対応した公開鍵に、自装置を認証する第三者が署名を付与した公開鍵証明書と該秘密鍵による署名を前記第２の装置に転送するプロセスを有し、

前記第２の装置に搭載される、

前記公開鍵証明書を検証して署名者の公開鍵を特定するプロセスと、

１乃至複数のフィガープリントを保持または、入手するプロセスとを更に有し、

前記第１の認証プロセスは、

前記秘密鍵による署名を前記公開鍵証明書が含む公開鍵により検証し、かつ、該公開鍵証明書の署名者の公開鍵の一方向関数による出力が、保持されている前記フィンガープリントに含まれることを検証することにより、転送元の前記第１の装置を認証するプロセスを含む請求項１８記載の原本データ流通プログラムを格納した記憶媒体。

【請求項２４】　前記第２の装置に搭載される、

前記第１の情報と、１乃至複数の第１の装置に対応する情報とを対応付ける利用者信任情報を保持もしくは、入手するプロセスを有し、

前記第１の認証プロセスは、

転送された前記原本性情報の第１の情報から、保持されている前記利用者信任情報を用いて、該第１の情報に対応する第１の装置に対応する情報を抽出し、転送元装置が該利用者信任情報から抽出された第１の装置に含まれることを検証することにより、該転送元の第１の装置を認証するプロセスを含む請求項１８記載の原本データ流通プログラムを格納した記憶媒体。

【請求項２５】　前記第２の装置に搭載される、

前記第１の情報と前記第２の情報から、１乃至複数の前記第１の装置に対応する情報を対応付ける利用者信任情報を保持もしくは、入手するプロセスを有し、

前記第１の認証プロセスは、

転送された前記原本性情報の第１の情報と第２の情報とから、保持されている前記利用者信任情報を用いて、該第１の情報と該第２の情報に対応する第１の装置に対応する情報を抽出し、転送元装置が、該利用者信任情報から抽出された第１の装置に含まれることを検証することにより、該転送元の第１の装置を認証するプロセスを含む請求項１８記載の原本データ流通プログラムを格納した記憶媒体。

【請求項２６】　電子的な情報である原本データの蓄積や流通を行う発行者装置に搭載される原本データ流通プログラムを格納した記憶媒体であって、

前記発行者装置に対応する情報を第１の情報とし、あるデータもしくは、該データに対応する情報を第２の情報として、原本性情報を生成する原本性情報生成プロセスと、

前記原本性情報を転送する原本性情報転送プロセスとを有することを特徴とする原本データ流通プログラムを格納した記憶媒体。

【請求項２７】　秘密鍵を秘匿するプロセスと、

前記秘密鍵に対応する公開鍵の一方向関数による出力である自装置のフィンガープリントを前記第１の情報として生成するプロセスを有する請求項２６記載の原本データ流通プログラムを格納した記憶媒体。

【請求項２８】　前記原本性情報の前記第２の情報として、データの一方向関数による出力を生成するプロセスを有する請求項２６記載の原本データ流通プログラムを格納した記憶媒体。

【請求項２９】　前記原本性情報の前記第２の情報として、ネットワーク上の資源の識別子を用いるプロセスを含む請求項２８記載の原本データ流通プログラムを格納した記憶媒体。

【請求項３０】　電子的な情報である原本データの蓄積や流通を行う利用者装置に搭載される原本データ流通プログラムを格納した記憶媒体であって、

ある装置に対応する第１の情報と、データもしくは、データに対応する情報である第２の情報から構成される原本性情報を転送する原本性情報転送プロセスと、

他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定

する特定プロセスと、

前記転送元装置が認証された場合、もしくは、該転送元装置と前記原本性情報の第１の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する認証プロセスと、

前記認証プロセスで前記原本性情報が有効であると判別された場合に、該原本性情報を格納する格納プロセスとを有することを特徴とする原本データ流通プログラムを格納した記憶媒体。

【請求項３１】　前記利用者装置から前記原本性情報を転送する際に、該原本性情報を消去するプロセスを有する請求項３０記載の原本データ流通プログラムを格納した記憶媒体。

【請求項３２】　電子的な情報である原本データの蓄積や流通を行う改札者装置に搭載される原本データ流通プログラムであって、

原本性情報の転送元装置を特定する特定プロセスと、

前記転送元装置を認証する認証プロセスと、

前記認証プロセスにおいて、自装置に転送された前記原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第２の情報に対応するデータに対応する処理を行うデータ処理プロセスを有することを特徴とする原本データ流通プログラムを格納した記憶媒体。

【請求項３３】　発行者装置に対応する情報である発行者情報を保持もしくは、入手するプロセスを更に有し、

前記データ処理プロセスは、

前記認証プロセスにおいて、転送された前記原本性情報が有効であると判別され、かつ、該原本性情報の装置に対応する第１の情報に対応する発行者装置が、保持されている前記発行者情報に対応する発行者装置に含まれる場合に、該原本性情報のデータまたは、データに対応する情報である第２の情報に対応するデータに対する処理を行う請求項３２記載の原本データ流通プログラムを格納した記憶媒体。

【請求項３４】　電子的な情報である原本データの蓄積や流通を行う原本データ流通プログラムを格納した記憶媒体であって、

発行者装置に搭載される、

前記発行者装置に対応する情報を第１の情報とし、あるデータもしくは、該データに対応する情報を第２の情報として、原本性情報を生成する第１の原本性情報生成プロセスと、

前記原本性情報を転送する第１の原本性情報転送プロセスと、

利用者装置に搭載される、

ある装置に対応する第１の情報と、データもしくは、データに対応する情報である第２の情報から構成される原本性情報を転送する第２の原本性情報転送プロセスと、

他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する第１の特定プロセスと、

前記転送元装置が認証された場合、もしくは、該転送元装置と該原本性情報の第１の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する第１の認証プロセスと、

前記第１の認証プロセスで該原本性情報が有効であると判別された場合に、該原本性情報を格納する格納プロセスと、

改札者装置に搭載される、

原本性情報の転送元装置を特定する第２の特定プロセスと、

前記転送元装置を認証する第２の認証プロセスと、

前記第２の認証プロセスにおいて、前記改札者装置に転送された該原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第２の情報に対応するデータに対する処理を行うデータ処理プロセスとを有することを特徴とする原本データ流通プログラムを格納した記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、原本データ流通システム及び原本データ流通プログラムを格納した記憶媒体に係り、特に、電子チケットなどの権利を表象するデータやディジタル著作物など、有効な複製数を一定数以下に保つことが必要とされるデータについ

て、蓄積や配送のための手段を提供するための原本データ流通システム及び原本データ流通プログラムを格納した記憶媒体に関する。

【０００２】

【従来の技術】

権利を表象したデータや著作物などは、配布者などの意図する数を越えて同時に複製が存在することを防止することが求められる。即ち、配布したデータが利用者などにより複製され、それらが多重に利用されることを防ぐ必要がある。

従来は、以下で示すような技術によりそのような多重利用を防止している。

【０００３】

第１の方法として、権利を表象するデータについて、権利の提供者などにより該データの使用履歴を保持しておき、権利の行使時に、当該データが既に使用されていないかどうかを検証する。もし、既に使用されていれば、当該データが表象する権利の行使を拒否する。

第２の方法として、データ自身を耐タンパ装置に格納し、当該データを当該耐タンパ装置の外からは参照できないようにする。権利の行使時には、当該データを該耐タンパ装置より抹消する。

【０００４】

第３の方法として、データ自身は通常の蓄積媒体に格納するが、当該データの原本性を示すデータ（トークン）のみを耐タンパ装置に格納する。権利の行使時には、そのトークンを当該耐タンパ装置より抹消する。

【０００５】

【発明が解決しようとする課題】

しかしながら、上記従来の第１の方法では、耐タンパ装置など特別な装置を必要としていないが、該データを転々と流通させる際には、問題が生じる。すなわ、当該技術では、行使時の事後検出しか行えないため、流通過程では、当該データの有効性は判定できないという問題がある。

【０００６】

従来の第２の方法では、耐タンパ装置を用いることにより、データの唯一性を保証することができる。また、「特表平６－５０３９１３」や「特表平９－５１

１３５０」などで述べられている方式などを併用し、暗号によって保護された安全な通信路を介して耐タンパ装置を結合し、当該通信路を介してデータの授受を行うことにより、該データの流通を、複製を事前防止しながら行うことが可能とする。しかしながら、当該技術は、耐タンパ装置の中にデータを格納する必要があるため、以下の２点が問題となる。

【０００７】

まず、データの記述そのものを見ることができなくなるため、記述の正当性の検証など、複製に関する有効性以外の検証も全て該タンパ装置に委ねなければならないという制約が生ずる。

また、データの格納部のみならず、データの取扱に必要な処理も全て耐タンパ装置が負わなければならいなため、耐タンパ装置に対して記憶容量や処理速度に大きな要求が発生する。特に、現時点で耐タンパ装置として一般的なＩＣカードでは、処理速度や記憶容量に不足が生じる。

【０００８】

従来の第３の方法は、原本性を示すデータであるトークンのみを耐タンパ装置に格納することにより、データの有効な複製数を常に一定以下に保つことを保証しつつ、記述の正当性の検証を含む複製に関する有効性以外の検証を全て耐タンパ装置に委ねることなく、処理速度や記憶容量等の処理負荷を低減させる（特願平１１－３９０８０）。しかしながら、該技術では、実用上主に、以下の２点が問題となる。

【０００９】

まず、トークンの生成時に、データと該データに付与された署名を検証するためにデータ及び該データの署名を耐タンパ装置に転送しなくてはならず、その一方で、ＩＣカードの転送速度は、９６００bit/s 程度（ＩＳＯ－７８１６）と比較的低速であるため、耐タンパ装置としてＩＣカードを用いると、該データの大きさによってはトークンの生成に要する時間を著しく増大させる。

【００１０】

また、当該技術では、データに対して署名を付与したものに対してトークンを生成し、消費の際にも該データ及び該署名を用いてトークンの検証が必要となる

ため、該データのみならず、該署名も共に流通させる必要が生じ、これは、システムに構築のために必要な記憶容量や流通の際の処理時間を増大させる。

本発明は、上記の点に鑑みなされたもので、従来の第３の方法におけるトークンの生成やデータの流通などにおける負荷を低減する原本データ流通システム及び原本データ流通プログラムを格納した記憶媒体を提供することを目的とする。

【００１１】

【課題を解決するための手段】

本発明（請求項１）は、電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、

ある装置に対応する第１の情報と、データもしくは、データに対応する情報である第２の情報と、から構成される原本性情報を転送する転送手段を有する第１の装置と、

原本性情報の転送元装置を特定する特定手段と、該転送元装置が認証された場合に該原本性情報を有効であると判別する第１の認証手段と、該転送元装置と該原本性情報の第１の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判別する第２の認証手段とを有する第２の装置とを有する。

【００１２】

本発明（請求項２）は、第１の装置において、

秘密鍵を秘匿する手段を更に有し、

第２の装置において、

１乃至、複数の秘密鍵に対応する公開鍵の一方向関数による出力である自装置のフィンガープリントを保持、または、入手する手段を更に有し、

第２の装置の第１の認証手段において、

転送元の第１の装置がフィンガープリントに対応する秘密鍵を保持していることを検証することにより、該転送元の第１の装置を認証する。

【００１３】

本発明（請求項３）は、第１の装置の転送手段において、

当該第１の装置が１乃至複数の第三者によって認証されていることを証明する情報であり、該第三者である認証者に対応する情報である第三者証明を第２の装

置に転送する手段を有し、

第２の装置において、

１乃至複数の第三者に対応する第三者情報を保持、または、入手する手段を有し、

当該第２の装置の第１の認証手段において、

転送元装置である第１の装置が第三者証明における認証対象であり、かつ、該第三者証明の認証者のいずれかが、保持されている第三者情報に対応する第三者に含まれることを検証することにより、該転送元の第１の装置を認証する。

【００１４】

本発明（請求項４）は、第２の装置において、

第１の情報と、１乃至複数の第三者に対応する情報とを対応付ける第三者信任情報を保持もしくは、入手する手段を有し、

当該第２の装置の第１の認証手段において、

原本性情報の転送元である第１の装置が該第三者証明における認証対象であり、かつ、転送された原本性情報の第１の情報から、保持されている第三者信任情報を用いて該第１の情報に対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信任情報から抽出された第三者に含まれることを検証することにより、該転送元の第１の装置を認証する。

【００１５】

本発明（請求項５）は、第２の装置において、

第１の情報と第２の情報とから、第三者に対応する情報とを対応づける、第三者信任情報を保持もしくは、入手する手段を有し、

当該第２の装置の第１の認証手段において、

転送された原本性情報の第１の情報と第２の情報から、第三者信任情報を用いて該第１の情報と該第２の情報の対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信任情報から抽出された第三者に含まれることを検証することにより、該転送元の第１の装置を認証する。

【００１６】

本発明（請求項６）は、第１の装置において、

秘密鍵を秘匿する手段と、

秘密鍵に対応した公開鍵に、自装置を認証する第三者が署名を付与した公開鍵証明書と該秘密鍵による署名を第２の装置に転送する手段を有し、

第２の装置において、

公開鍵証明書を検証して署名者の公開鍵を特定する手段と、

１乃至複数のフィガープリントを保持または、入手する手段とを更に有し、

当該第２の装置の第１の認証手段において、

秘密鍵による署名を公開鍵証明書が含む公開鍵により検証し、かつ、該公開鍵証明書の署名者の公開鍵の一方向関数による出力が、保持されているフィンガープリントに含まれることを検証することにより、転送元の第１の装置を認証する。

【００１７】

本発明（請求項７）は、第２の装置において、

第１の情報と、１乃至複数の第１の装置に対応する情報とを対応付ける利用者信任情報を保持もしくは、入手する手段を有し、

第１の認証手段において、

転送された原本性情報の第１の情報から、保持されている利用者信任情報を用いて、該第１の情報に対応する第１の装置に対応する情報を抽出し、転送元装置が該利用者信任情報から抽出された第１の装置に含まれることを検証することにより、該転送元の第１の装置を認証する。

【００１８】

本発明（請求項８）は、第２の装置において、

第１の情報と第２の情報から、１乃至複数の第１の装置に対応する情報を対応付ける利用者信任情報を保持もしくは、入手する手段を有し、

第１の認証手段において、

転送された原本性情報の第１の情報と第２の情報とから、保持されている利用者信任情報を用いて、該第１の情報と該第２の情報に対応する第１の装置に対応する情報を抽出し、転送元装置が、該利用者信任情報から抽出された第１の装置に含まれることを検証することにより、該転送元の第１の装置を認証する。

【００１９】

本発明（請求項９）は、電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、

自装置に対応する情報を第１の情報とし、あるデータもしくは、該データに対応する情報を第２の情報として、原本性情報を生成する原本性情報生成手段と、

原本性情報を転送する原本性情報転送手段とを有する発行者装置を有する。

【００２０】

本発明（請求項１０）は、発行者装置において、

秘密鍵を秘匿する手段と、

秘密鍵に対応する公開鍵の一方向関数による出力である自装置のフィンガープリントを第１の情報として生成する手段を有する。

本発明（請求項１１）は、発行者装置において、

原本性情報の第２の情報として、データの一方向関数による出力を生成する手段を有する。

【００２１】

本発明（請求項１２）は、発行者装置において、

原本性情報の第２の情報として、ネットワーク上の資源の識別子を用いる。

本発明（請求項１３）は、電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、

ある装置に対応する第１の情報と、データもしくは、データに対応する情報である第２の情報から構成される原本性情報を転送する原本性情報転送手段と、

他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する特定手段と、

転送元装置が認証された場合、もしくは、該転送元装置と該原本性情報の第１の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する認証手段と、

認証手段で原本性情報が有効であると判別された場合に、該原本性情報を格納する格納手段とを有する利用者装置を有する。

【００２２】

本発明（請求項１４）は、利用者装置において、

自装置から原本性情報を転送する際に、該原本性情報を消去する手段を有する。

本発明（請求項１５）は、電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、

原本性情報の転送元装置を特定する特定手段と、

転送元装置を認証する認証手段と、

認証手段において、自装置に転送された原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第２の情報に対応するデータに対応する処理を行うデータ処理手段を有する改札者装置を有する。

【００２３】

本発明（請求項１６）は、改札者装置において、

発行者装置に対応する情報である発行者情報を保持もしくは、入手する手段を更に有し、

データ処理手段において、

認証手段において転送された原本性情報が有効であると判別され、かつ、該原本性情報の装置に対応する第１の情報に対応する発行者装置が、保持されている発行者情報に対応する発行者装置に含まれる場合に、該原本性情報のデータまたは、データに対応する情報である第２の情報に対応するデータに対する処理を行う。

【００２４】

図１は、本発明の原理構成図である。

本発明（請求項１７）は、電子的な情報である原本データの蓄積や流通を行う原本データ流通システムであって、

自装置に対応する情報を第１の情報とし、あるデータもしくは、該データに対応する情報を第２の情報として、原本性情報を生成する第１の原本性情報生成手段１１０と、該原本性情報を転送する第１の原本性情報転送手段１２０とを有する発行者装置１００と、

ある装置に対応する第１の情報と、データもしくは、データに対応する情報で

ある第２の情報から構成される原本性情報を転送する第２の原本性情報転送手段２１０と、他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する第１の特定手段２２０と、該転送元装置が認証された場合、もしくは、該転送元装置と該原本性情報の第１の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する第１の認証手段２３０と、該第１の認証手段２３０で該原本性情報が有効であると判別された場合に、該原本性情報を格納する格納手段２４０とを有する利用者装置２００と、

原本性情報の転送元装置を特定する第２の特定手段３１０と、転送元装置を認証する第２の認証手段３２０と、該第２の認証手段３２０において、自装置に転送された該原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第２の情報に対応するデータに対する処理を行うデータ処理手段３３０を有する改札者装置３００とを有する。

【００２５】

本発明（請求項１８）は、電子的な情報である原本データの蓄積や流通を行う原本データ流通プログラムを格納した記憶媒体であって、

第１の装置に搭載される、

ある装置に対応する第１の情報と、データもしくは、データに対応する情報である第２の情報と、から構成される原本性情報を転送させる転送プロセスと、

第２の装置に搭載される、

原本性情報の転送元装置を特定する特定プロセスと、該転送元装置が認証された場合に該原本性情報を有効であると判別する第１の認証プロセスと、該転送元装置と該原本性情報の第１の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判別する第２の認証プロセスとを有する。

【００２６】

本発明（請求項１９）は、第１の装置に搭載される、秘密鍵を秘匿するプロセスを更に有し、

第２の装置に搭載される、

１乃至、複数の秘密鍵に対応する公開鍵の一方向関数による出力である自装置のフィンガープリントを保持、または、入手するプロセスを更に有し、

第１の認証プロセスにおいて、

転送元の第１の装置がフィンガープリントに対応する秘密鍵を保持していることを検証することにより、該転送元の第１の装置を認証するプロセスを含む。

【００２７】

本発明（請求項２０）は、第１の装置に搭載されるの転送プロセスにおいて、

自装置が１乃至複数の第三者によって認証されていることを証明する情報であり、該第三者である認証者に対応する情報である第三者証明を第２の装置に転送するプロセスを有し、

第２の装置に搭載される、

１乃至複数の第三者に対応する第三者情報を保持、または、入手するプロセスを有し、

第２の装置に搭載される第１の認証プロセスにおいて、

転送元装置である第１の装置が第三者証明における認証対象であり、かつ、該第三者証明の認証者のいずれかが、保持されている第三者情報に対応する第三者に含まれることを検証することにより、該転送元の第１の装置を認証するプロセスを含む。

【００２８】

本発明（請求項２１）は、第２の装置に搭載される、

第１の情報と、１乃至複数の第三者に対応する情報とを対応付ける第三者信任情報を保持もしくは、入手するプロセスを有し、

第２の装置に搭載される第１の認証プロセスにおいて、

原本性情報の転送元である第１の装置が該第三者証明における認証対象であり、かつ、転送された原本性情報の第１の情報から、保持されている第三者信任情報を用いて該第１の情報に対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信任情報から抽出された第三者に含まれることを検証することにより、該転送元の第１の装置を認証するプロセスを含む。

【００２９】

本発明（請求項２２）は、第２の装置に搭載される、

第１の情報と第２の情報とから、第三者に対応する情報とを対応づける、第三

者信任情報を保持もしくは、入手するプロセスを有し、

第２の装置に搭載される第１の認証プロセスにおいて、

転送された原本性情報の第１の情報と第２の情報から、第三者信任情報を用いて該第１の情報と該第２の情報の対応する第三者に対応する情報を抽出し、該第三者証明の認証者のいずれかが、該第三者信任情報から抽出された第三者に含まれることを検証することにより、該転送元の第１の装置を認証するプロセスを含む。

【００３０】

本発明（請求項２３）は、第１の装置に搭載される、

秘密鍵を秘匿するプロセスと、

秘密鍵に対応した公開鍵に、自装置を認証する第三者が署名を付与した公開鍵証明書と該秘密鍵による署名を第２の装置に転送するプロセスを有し、

第２の装置に搭載される、

公開鍵証明書を検証して署名者の公開鍵を特定するプロセスと、

１乃至複数のフィガープリントを保持または、入手するプロセスとを更に有し、

第２の装置に搭載される第１の認証プロセスにおいて、

秘密鍵による署名を公開鍵証明書が含む公開鍵により検証し、かつ、該公開鍵証明書の署名者の公開鍵の一方向関数による出力が、保持されているフィンガープリントに含まれることを検証することにより、転送元の第１の装置を認証するプロセスを含む。

【００３１】

本発明（請求項２４）は、第２の装置に搭載される、

第１の情報と、１乃至複数の第１の装置に対応する情報とを対応付ける利用者信任情報を保持もしくは、入手するプロセスを有し、

第２の装置に搭載される第１の認証プロセスにおいて、

転送された原本性情報の第１の情報から、保持されている利用者信任情報を用いて、該第１の情報に対応する第１の装置に対応する情報を抽出し、転送元装置が該利用者信任情報から抽出された第１の装置に含まれることを検証することに

より、該転送元の第１の装置を認証するプロセスを含む。

【００３２】

本発明（請求項２５）は、第２の装置に搭載される、

第１の情報と第２の情報から、１乃至複数の第１の装置に対応する情報を対応付ける利用者信任情報を保持もしくは、入手するプロセスを有し、

第２の装置に搭載される第１の認証プロセスにおいて、

転送された原本性情報の第１の情報と第２の情報とから、保持されている利用者信任情報を用いて、該第１の情報と該第２の情報に対応する第１の装置に対応する情報を抽出し、転送元装置が、該利用者信任情報から抽出された第１の装置に含まれることを検証することにより、該転送元の第１の装置を認証するプロセスを含む。

【００３３】

本発明（請求項２６）は、電子的な情報である原本データの蓄積や流通を行う発行者装置に搭載される原本データ流通プログラムを格納した記憶媒体であって、

発行者装置に対応する情報を第１の情報とし、あるデータもしくは、該データに対応する情報を第２の情報として、原本性情報を生成する原本性情報生成プロセスと、

原本性情報を転送する原本性情報転送プロセスとを有する。

【００３４】

本発明（請求項２７）は、秘密鍵を秘匿するプロセスと、

秘密鍵に対応する公開鍵の一方向関数による出力である発行者装置のフィンガープリントを第１の情報として生成するプロセスを有する。

本発明（請求項２８）は、原本性情報の第２の情報として、データの一方向関数による出力を生成するプロセスを有する。

【００３５】

本発明（請求項２９）は、原本性情報の第２の情報として、ネットワーク上の資源の識別子を用いるプロセスを含む。

本発明（請求項３０）は、電子的な情報である原本データの蓄積や流通を行う

利用者装置に搭載される原本データ流通プログラムを格納した記憶媒体であって、

ある装置に対応する第１の情報と、データもしくは、データに対応する情報である第２の情報から構成される原本性情報を転送する原本性情報転送プロセスと、

他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する特定プロセスと、

転送元装置が認証された場合、もしくは、該転送元装置と該原本性情報の第１の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する認証プロセスと、

認証プロセスで原本性情報が有効であると判別された場合に、該原本性情報を格納する格納プロセスとを有する。

【００３６】

本発明（請求項３１）は、利用者装置から原本性情報を転送する際に、該原本性情報を消去するプロセスを有する。

本発明（請求項３２）は、電子的な情報である原本データの蓄積や流通を行う改札者装置に搭載される原本データ流通プログラムであって、

原本性情報の転送元装置を特定する特定プロセスと、

転送元装置を認証する認証プロセスと、

認証プロセスにおいて、自装置に転送された原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第２の情報に対応するデータに対応する処理を行うデータ処理プロセスを有する。

【００３７】

本発明（請求項３３）は、発行者装置に対応する情報である発行者情報を保持もしくは、入手するプロセスを更に有し、

データ処理プロセスにおいて、

認証プロセスにおいて、転送された原本性情報が有効であると判別され、かつ、該原本性情報の装置に対応する第１の情報に対応する発行者装置が、保持されている発行者情報に対応する発行者装置に含まれる場合に、該原本性情報のデー

タまたは、データに対応する情報である第２の情報に対応するデータに対する処理を行う。

【００３８】

本発明（請求項３４）は、電子的な情報である原本データの蓄積や流通を行う原本データ流通プログラムを格納した記憶媒体であって、

発行者装置に搭載される、

発行者装置に対応する情報を第１の情報とし、あるデータもしくは、該データに対応する情報を第２の情報として、原本性情報を生成する第１の原本性情報生成プロセスと、

原本性情報を転送する第１の原本性情報転送プロセスと、

利用者装置に搭載される、

ある装置に対応する第１の情報と、データもしくは、データに対応する情報である第２の情報から構成される原本性情報を転送する第２の原本性情報転送プロセスと、

他の装置から原本性情報が転送された際に、該原本性情報の転送元装置を特定する第１の特定プロセスと、

転送元装置が認証された場合、もしくは、該転送元装置と該原本性情報の第１の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判定する第１の認証プロセスと、

第１の認証プロセスで該原本性情報が有効であると判別された場合に、該原本性情報を格納する格納プロセスと、

改札者装置に搭載される、

原本性情報の転送元装置を特定する第２の特定プロセスと、

転送元装置を認証する第２の認証プロセスと、

第２の認証プロセスにおいて、改札者装置に転送された該原本性情報が有効であると判別された場合に、該原本性情報のデータまたは、データに対応する第２の情報に対応するデータに対する処理を行うデータ処理プロセスとを有する。

【００３９】

上記の請求項１及び請求項１８では、第１の装置は、装置を示す第１の情報と

データを示す第２の情報から構成される原本性情報を転送する手段を備え、第２の装置は、原本性情報の転送を受ける際に、第１の情報が示す装置が転送元装置であるか、もしくは、転送元装置が転送先装置にとって「信用できる」装置である場合のみ、原本性情報を有効であると判別することが可能となる。

【００４０】

請求項２及び請求項１９では、公開暗号系を用いて転送元装置を特定し、第２の装置が「信用する」利用者装置を示すフィンガープリントを用いて、転送元装置が信用できるかどうかを判断することが可能となる。

請求項３及び請求項２０では、第１の装置が、当該装置が第三者である認証者に「信用されている」ことを証明する情報である第三者情報を第２の装置に転送する手段を備え、第２の装置は、当該装置が「信用する」第三者を示す情報である第三者情報を保持する手段と、第１の装置から原本性情報が転送された際に、当該原本性情報の転送元装置が第１の装置であり、かつ、第２の装置が保持する第三者情報が示す第三者に、当該第三者証明の認証者が含まれることを検証することにより、信用できるかどうかを判断することが可能となる。

【００４１】

請求項４及び請求項２１では、発行者層が「信用する」第三者装置を示す第三者信任情報と、第１の装置が第三者である認証者により認証されていることを示す第三者証明を用い、転送元の第１の装置が第三者証明の認証者により認証された装置であり、かつ、該認証者が原本性情報の第１の情報が示す装置により信用されていることを利用者信任情報を用いて検証することにより、信用できる第１の装置を特定する情報を直接に指示することなく、信用できる第１の装置を発行者装置が指定することが可能となる。

【００４２】

請求項５及び請求項２２では、発行者装置が「信用する」第三者装置を示す第三者信任情報と、第１の装置が第三者である認証者により認証されていることを示す第三者証明を用い、転送元の第１の装置が当該第三者証明の認証者により認証された装置であり、かつ、当該認証者が原本性情報の第１の情報が示す装置により信用されていることを利用者信任情報を用いて検証することにより、信用で

きる第１の装置を特定する情報を直接に指定することなく、信用できる第１の装置を発行者装置がデータ毎、もしくは、データの集合毎に指定することが可能となる。

【００４３】

請求項６及び請求項２３では、公開鍵暗号系を用いて転送元装置を特定し、公開鍵証明書を用いて第三者証明を実現し、フィンガープリントを用いて第三者情報を実現し、原本性情報の転送元装置が第１の装置であり、かつ、第２の装置が保持する第三者情報を示す第三者に、第三者証明の認証者が含まれることを検証することにより、第１の装置を検証し、信用できる第１の装置を特定する情報を直接に保持することなく、第１の装置が信用できるかどうかを判断することが可能となる。

【００４４】

請求項７及び請求項２４では、発行者装置が「信用する」第１の装置を示す利用者信任情報を用い、転送元の第１の装置が原本性情報の第１の情報が示す装置により信用されていることを利用者信任情報を用いて検証することにより、信用できる第１の装置を発行者装置が指定することが可能となる。

請求項８及び請求項２５では、発行者装置がデータの流通に関して「信用する」第１の装置を示す利用者信任情報を用い、転送元の第１の装置が原本性情報の第１の情報が示す装置により信用されていることを利用者信任情報を用いて検証することにより、信用できる第１の装置を発行者装置がデータ毎、もしくは、データの集合毎に指定することが可能となる。

【００４５】

請求項９及び請求項２６では、原本性情報の第１の情報を自装置を示す情報として原本性を生成する手段と、生成した当該原本性情報を転送する手段を備えた発行者装置を提供することが可能となる。

請求項１０及び請求項２７では、発行者装置において、発行者装置の公開鍵のフィンガープリントを、原本性情報の第１の情報として用い、原本性情報を生成する。

【００４６】

請求項１１及び請求項２８では、発行者装置において、ＭＤ５やＳＨＡ－１などの一方向関数によるデータのダイジェスト値を、原本性情報の第２の情報として用い、原本性情報を生成する。

請求項１２及び請求項２９では、発行者装置において、ＵＲＬなどのネットワーク上の識別子を、原本性情報の第２の情報として用い、原本性情報を生成する。

【００４７】

請求項１３及び請求項３０では、利用者装置において、原本性情報を転送する手段と、有効性を判別する手段とを備え、有効な原本性情報のみを格納する手段を備える。

請求項１４及び請求項３１では、利用者装置において、原本性情報を転送する際に、格納された原本性情報を消去する。

【００４８】

請求項１５及び請求項３２では、改札者装置において、有効性を判別する手段と、データを処理する手段を備え、有効な原本性情報の第２の情報が示すデータを処理する手段を備える。

請求項１６及び請求項３３では、改札者装置において、「正しい」発行者を示す発行者情報を備え、有効性を検証された原本性情報の第１の情報を示す発行者が発行者情報が示す発行者に含まれた場合に、原本性情報の第２の情報が示すデータを処理する。

【００４９】

請求項１７及び請求項３４では、上記で述べた発行者装置と、利用者装置と、改札者装置を有するシステムを構成することにより、これらの装置間において、チケット発行、チケットの譲渡、チケットの消費及びチケットの提示等の各処理を行うことが可能となる。

【００５０】

【発明の実施の形態】

最初に、権利を表象する電子情報である電子チケットをデータとして用いる場合における、原本データ流通システムにおけるデータ蓄積システムについて説明

する。

図２は、本発明の原本データ流通システムにおけるデータ蓄積システムの構成を示す。

【００５１】

同図において、チケットの発行者は、発行者装置１を有し、チケットの発行先となる利用者は利用者装置２を有している。チケットの発行の際には、発行者装置１と利用者装置２の間は、接続装置４を介して通信手段が確立され、発行者装置１で有効化されたチケットを利用者装置２に転送する。

上記のこれらの装置は、図２（ａ），（ｂ）などの構成をとることができる。

【００５２】

同図（ａ）は、利用者装置２としてＩＣカードを用い、接続装置４としてＩＣカードリーダライタを用いる際の代表的な構成を示し、同図（ｂ）は、利用者装置としてＩＣカードなどの耐タンパ装置を装備可能もしくは、安全な場所に補間されたＰＣを用い、接続装置４としてネットワークを用いる際の代表的な構成を示す。なお、同図（ａ），（ｂ）の構成を混在させて用いることも可能である。

【００５３】

上記の通信手段は、チケットの発行の開始から終了までの間のみ確立させていればよい。以下、「譲渡」、「消費」、「提示」の際にもこれは同様である。

チケット譲渡の際には、発行時と同様に利用者装置２間で接続装置４を介して通信手段を確立し、有効なチケットを利用者装置２間で転送する。

チケットの改札者は、改札者装置３を有している。チケット消費の際には、発行時と同様に利用者装置２と改札者装置３との間で接続装置４を介して通信手段を確立し、利用者装置２から改札者装置３に有効なチケットを転送する。

【００５４】

チケット提示の際には、２つの利用者装置２の間、もしくは利用者装置２と改札者装置３との間で、接続装置４を介して通信手段を確立し、利用者装置２から他の利用者装置２もしくは、改札者装置３に有効なチケットを所持していることの証明を転送する。

このように、本発明に係るデータ蓄積システムは、一時的な相互通信手段を提

供する１つまたは、複数の接続装置４により接続された、１つまたは、複数の発行者装置１と、１つまたは、複数の利用者装置２と、１つまたは、複数の改札者装置３とから構成されるシステムである。

【００５５】

【実施例】

以下、図面と共に本発明の実施例を説明する。

図３から図６を用いて、上記のデータ蓄積システムを構成する各装置について説明する。

最初に、以下の説明で用いる式の意味を示す。

【００５６】

ｘ‖ｙとは、ｘとｙの連接である。

Ｈとは、一方向ハッシュ関数であり、ｙ＝Ｈ（ｘ）を満たすようなｘをｙから求めることが困難であるという性質を持つ。このようなハッシュ関数として、米ＲＳＡ社の「ＭＤ５」等が知られている。

S_{Pk}とは、検証関数V_{Pk}により検証可能な電子署名S_{Pk}（ｘ）を生成する署名関数である。

【００５７】

V_{Pk}は、検証関数であり、

$$V_{Pk}(x, S_{Pk}(x)) = 1,\ V_{Pk}(x, other) = 0$$
$$(other \neq S_{pk}(x))$$

という性質を持つ。即ち、電子署名S_{Pk}（ｘ）がｘに対するS_{Pk}による正しい署名であるかどうかを検証できる性質を持つ。

【００５８】

Ｐｋは、検証鍵であり、検証器ＶにＰｋを与えることにより、V_{Pk}を構成することが可能であるという性質を持つ。検証鍵Ｐｋ２及びS_{Pk1}によるＰｋ２の電子署名S_{Pk1}（Ｐｋ２）の組（Ｐｋ２，S_{Pk1}（Ｐｋ２））を特に、Ｐｋ１によるＰｋ２の鍵証明書と呼ぶ。また、Ｈ（Ｐｋ）を特に、Ｐｋのフィンガープリントと呼ぶ。

【００５９】

以上で述べたような性質を持つS_{Pk}, V_{Pk}を実現するような電子署名方式として、日本電信電話のＥＳＩＧＮなどが知られている。

図３は、本発明の一実施例の発行者装置の構成を示す。

図３に示す発行者装置１は、制御部１１、署名部１２、データ生成部１３、トークン生成部１４、信任情報生成部１５から構成される。

【００６０】

制御部１１は、検証鍵ＰｋＩを保持し、チケットの流通を安全に行うための制御を行う。ここで、ＰｋＩは、後述する署名部１２が備える署名関数S_{PkI}に対応する検証鍵であり、そのフィンガープリントＨ（ＰｋＩ）は、発行者を特定する識別子として用いられる。制御部１１による制御の詳細については、後述する。

【００６１】

署名部１２は、署名関数S_{PkI}を備える。S_{PkI}は、発行者装置１毎にそれぞれ異なり、署名部１２により秘匿される。

データ生成部１３は、内部で生成した情報に基づいて、もしくは、外部から与えられた情報に基づいて、データｍを生成する。本発明に係るデータ蓄積装置では、データｍの記述内容についてなんら制限を持つものではないため、データｍとして切符やコンサートチケットなどの一般的チケットによって扱われる権利を表象する電子情報のほか、プログラム、音楽、画像データなどを扱うことが可能である。

【００６２】

トークン生成部１４は、一方向ハッシュ関数Ｈを備え、データｍ及び検証鍵ＰｋＩよりトークン

$$(c_1, c_2) = (H(m) . H(PkI))$$

を生成する。ここで、c_2は、トークン発行者情報であり、当該トークンの発行者を特定するフィンガープリントである。ここでは、c_1にデータｍのハッシュ値を用いたが、これにはｍを識別する識別子などを用いることも可能である。

【００６３】

信任情報生成部１５は、信任情報（t_1, t_2, t_3）を生成する。（t_1,

t_2，t_3）は、署名部１２を用いて例えば、以下のように構成される。

$t_1 = \{H(PkA_1), H(PkA_2), \cdots, H(PkA_n)\}$

$t_2 = S_{PkI}(H(PkA_1) \| H(PkA_2) \| \cdots \| H(PkA_n))$

$t_3 = PkI$

ここで、$H(PkA_i)$は、発行者が「信用する」第三者（後述）を特定するフィンガープリントである。

【００６４】

ここで、信任情報は以下で示す（t'_1，t'_2，t'_3，t'_4）のように構成することも可能である。

$t'_1 = \{H(PkA_1), H(PkA_2), \cdots, H(PkA_n)\}$

$t'_2 = H(m)$

$t'_3 = S_{PkI}(H(PkA_1) \| H(PkA_2) \| \cdots \| H(PkA_n) \| H(m))$

$t'_4 = PkI$

この場合、$H(PkA_i)$は、発行者が「データｍを流通させるにあたって信用するに足りる」第三者を特定するフィンガープリントである。

【００６５】

また、上記信任情報は、第三者がさらに信任情報を発行することにより再帰的に構築することも可能である。

また、さらに、信任情報を各発行者が生成することをせず、後述する利用者装置の耐タンパ装置の制御部や、改札者装置の制御部が予め固定的に保持しておく形態を採ることも可能である。この場合、署名は必要なく、以下で示す（t''_1，t''_2）もしくは、t''_1のみとして信任情報を構成できる。

【００６６】

$t''_1 = \{H(PkA_1), H(PkA_2), \cdots, H(PkA_n)\}$

$t''_2 = H(m)$

この場合、$H(PkA_i)$は、当該制御部（を作成した第三者）が、「（データｍを流通させるにあたって）信用する」第三者を特定するフィンガープリントである。

【００６７】

以下においては、信任情報は（t_1，t_2，t_3）と構成されるものとして説明するが、上記のいずれの信任情報を用いる場合も容易に類推可能である。

図４は、本発明の一実施例の利用者装置の構成を示す。

同図に示す利用者装置２は、制御部２１、格納部２２と、制御部２３、認証部２４、署名部２５、番号生成部２６、格納部２７から構成される耐タンパ装置２８を有する。耐タンパ装置２８は、各構成部の機能や内容が改竄されることを（利用者本人からも）防止する。このような耐タンパ装置２８として、ＩＣカードや、ネットワーク経由で接続され、第三者により厳重に管理されたサーバなどが利用可能である。

【００６８】

制御部２１は、発行者情報

$$I_U = \{H(PkI_1), H(PkI_2), \cdots, H(PkI_n),\}$$

を備え、耐タンパ装置２８に封入された制御部２３と共に、チケットの流通を安全に行うための制御を行う。ここで、I_U は、利用者から「信用された」発行者を示す集合であり、当該利用者により任意の時点で更新可能である。制御部２１は、I_U に含まれる発行者により発行されたトークンのみを有効であると判断する。制御部２１による制御の詳細については、後述する。

【００６９】

格納部２２は、利用者が保持するデータの集合M_U 及び信任情報の集合T_U を格納する。これらの集合は、制御部２１により更新可能である。

制御部２３は、検証鍵ＰｋＵ，ＰｋＡ及び鍵証明書（ＰｋＵ，S_{PkA}（ＰｋＵ））を保持し、制御部２１と共に、チケットの流通を安全に行うための制御を行う。ここで、ＰｋＵは、署名部２５が備えるS_{PkU} に対応する検証鍵であり、そのフィンガープリントＨ（ＰｋＵ）は、該利用者装置を特定する識別子として用いる。S_{PkA} は、ＩＣカード製造者もしくは耐タンパサーバ管理者など、耐タンパ装置２８の安全性を保証する第三者により秘匿される署名関数である。すなわちS_{PkU} を含む耐タンパ装置２８は、S_{PkA} を保持する第三者により耐タンパ性を保証されている。制御部２３による制御の詳細については後述する。また、Ｐ

ｋＡは、S_{PkU} の検証鍵である。

【００７０】

認証部２４は、検証器Ｖを備える。

署名部２５は、署名関数S_{PkU} を備える。S_{PkU} は、利用者装置２毎にそれぞれ異なり、署名部２５により秘匿される。

番号生成部２６は、次番号r_U を保持し、番号の払出しを要求されると当該時点のr_U の値を返却すると共にr_U をインクリメントする。ここで、r_U は正数である。

【００７１】

格納部２７は、トークンの集合C_U 及び番号の集合R_U を格納する。これらの集合は、制御部２３により更新可能である。

図５は、本発明の一実施例の改札者装置の構成を示す。

制御部３１は、検証鍵ＰｋＥ及び、発行者情報

$$I_E = \{H(PkI_1), H(PkI_2), \cdots, H(PkI_n), \}$$

を備え、チケットの流通を安全に行うための制御を行う。ここで、I_E は、改札者から「信用された」発行者を示す集合であり、当該改札者により任意の時点で更新可能である。制御部３１は、I_E に含まれる発行者により発行されたトークンのみを正当と判断し、当該トークンを伴うチケットの消費に対してのみサービスを提供する。制御部３１による制御の詳細については後述する。

【００７２】

認証部３２は、検証器Ｖを備える。

番号生成部３３は、次番号r_E を保持し、番号の払出しを要求されると該時点のr_E を返却すると共に、r_E をインクリメントする。ここで、r_E は正数である。

格納部３４は、番号の集合R_E を格納する。これらの集合は、制御部３１により更新可能である。

【００７３】

図６は、本発明の一実施例の接続装置の構成を示す。

同図によれば、接続装置４は、通信部４１から構成される。

通信部４１は、発行者装置１、利用者装置２、改札者装置３間や、利用者装置２相互間での、一時的もしくは永続的な通信手段を提供する。ここで、接続装置４として、ＩＣカード挿入口を備えたキオスク端末や、ネットワークを介して相互接続された複数のＰＣ（パーソナルコンピュータ）などが利用可能である。

【００７４】

上述したような構成を有する各装置１～４を用いて電子チケットの流通を安全に行う方式を以下（１）チケットの発行の場合、（２）チケットの譲渡の場合、（３）チケットの検証の場合、のそれぞれの場合に分けて説明する。なお、各装置を跨がるそれぞれの通信は、接続装置４中の通信部４１を介するものとする。

（１）　チケット発行の場合：

図７は、本発明の一実施例のチケット発行の場合の動作を示すシーケンスチャートである。なお、同図では、発行者装置１と利用者装置２との間に存在する接続装置４は省略してある。

【００７５】

ステップ１０１）　発行者装置１の制御部１１は、データ生成部１３により、データｍを生成する。当該データｍを権利情報が記述されたチケットであるとする。

ステップ１０２）　発行者装置１の制御部１１は、トークン生成部１４にｍおよびＰｋＩを与え、トークン（c_1，c_2）＝（Ｈ（ｍ），Ｈ（ＰｋＩ））を生成する。

【００７６】

ステップ１０３）　制御部１１は、信任情報生成部１５により、信任情報（t_1，t_2，t_3）を生成する。信任情報の構成は前述の通りである。

ステップ１０４）　制御部１１は、利用者装置２の制御部２１にｍと（t_1，t_2，t_3）を転送する。

ステップ１０５）　利用者装置２の制御部２１は、ｍを格納部２２のM_Uに、（t_1，t_2，t_3）を格納部２２のT_Uに、それぞれ追加して格納する。

【００７７】

ステップ１０６）　制御部２１は、耐タンパ装置２８の制御部２３にセッショ

ン情報（s_1，s_2）の生成を依頼し、制御部２３は、以下の手順により（s_1，s_2）を生成し、制御部２１に転送する。

（ａ）　耐タンパ装置２８の番号生成部２６により番号r_Uの払出しを受ける。

【００７８】

（ｂ）　r_Uを格納部２７の番号集合R_Uに追加する。

（ｃ）　（s_1，s_2）＝（Ｈ（ＰｋＵ），r_U）を生成する。ここで、ＰｋＵは、制御部２１が保持する検証鍵である。

ステップ１０７）　制御部２１は、発行者装置１の制御部１１に（s_1，s_2）を転送する。

【００７９】

ステップ１０８）　発行者装置１の制御部１１は、署名部１２が備えるS_{PkI}と制御部１１が保持する検証鍵ＰｋＩを用い、トークン交換形式ｅ＝（e_1，e_2，e_3，e_4，e_5，e_6，e_7，e_8）を得る。ここで、ｅの各要素は、以下の値となる。また、チケット発行の際においてはe_7及びe_8はダミーであり、それぞれ任意の値を持たせてよい。

【００８０】

$e_1 = c_1$

$e_2 = c_2$

$e_3 = s_1$

$e_4 = s_2$

$e_5 = S_{PkI}$（$c_1 \| c_2 \| s_1 \| s_2$）

$e_6 =$ ＰｋＩ

$e_7 =$ ａｎｙ（任意）

$e_8 =$ ａｎｙ（任意）

ステップ１０９）　発行者装置１の制御部１１は、利用者装置２の制御部２１にｅを転送する。

【００８１】

ステップ１１０）　利用者装置２の制御部２１は、耐タンパ装置２８の制御部

２３にｅを転送し、ｅ内のトークンの格納を依頼する。

ステップ１１１）　耐タンパ装置２８の制御部２３は、認証部２４を用いて、以下の式の全てが成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部２１を介して、発行者装置１の制御部１１に処理を中断を通知する。

【００８２】

$$e_3 = H(PkU) \quad (1)$$

$$e_4 \in R_U \quad (2)$$

$$V_{e6}(e_1 \| e_2 \| e_3 \| e_4, e_5) = 1 \quad (3)$$

$$e_2 = H(e_6) \quad (4)$$

上記の式（１）及び式（２）は、セッション情報の正当性の検証である。この検証により、当該利用者装置２以外に宛られたトークン交換形式を格納すること、及びトークン交換形式の再利用によってトークンを複製すること、などによる不正を防止する。

【００８３】

式（３）は、トークン交換形式に対する署名の正当性の検証であり、この検証によりトークン交換形式の改竄を防止する。

また、式（４）は、トークン発行者情報の正当性の検証であり、当該トークンの署名者以外が発行者となるトークンを格納することを防止する。

ステップ１１２）　利用者装置２の耐タンパ装置２８の制御部２３は、格納部２７のR_Uからe_4（$=r_U$）を削除する。

【００８４】

ステップ１１３）　耐タンパ装置２８の制御部２３は、格納部２７のC_Uに（e_1，e_2）を追加する。

ステップ１１４）　耐タンパ装置２８の制御部２４は、制御部２１に（e_1，e_2）を転送し、処理の正常終了を通知する。

ステップ１１５）　制御部２１は、以下の式が成立することを検証する。検証に失敗した場合は、処理の中断を、検証に成功した場合は処理の正常終了を、発行者装置１の制御部１１に通知する。

【００８５】

$$e_1 = H(m) \qquad (5)$$

$$e_2 \in I_U \qquad (6)$$

式（５）及び式（６）は、転送されたトークンが、対象とするチケットに対応し、正当な発行者によって発行されたものであることの検証である。この検証により、発行されたチケットが有効であることを確認する。

【００８６】

（２）　チケット譲渡の場合：

以下は、利用者装置２ａから利用者装置２ｂに対する、接続装置４を介したチケット譲渡処理の流れである。

図８、図９は、本発明の一実施例のチケット譲渡の場合の動作を示すシーケンスチャートである。なお、同図において２つの利用者装置２ａ，２ｂの間に存在する接続装置４は省略してある。また、利用者装置２ａの各構成要素の各々にはａを付し、利用者装置２ｂの各構成要素の各々にはｂを付す。

【００８７】

ステップ２０１）　利用者装置２ａの制御部２１ａは、格納部２２ａが保持するM_{Ua}から譲渡対象となるチケットｍを抽出する。

ステップ２０２）　利用者装置２ａの制御部２１ａは、格納部２２ａが保持するT_{Ua}からｍの発行者による信任情報（t_1，t_2，t_3）を抽出する。

ステップ２０３）　制御部２１ａは、利用者装置２ｂの制御部２１ｂにｍと（t_1，t_2，t_3）を転送する。

【００８８】

ステップ２０４）　利用者装置２ｂの制御部２１ｂは、ｍを格納部２２ｂのM_{Ub}に、（t_1，t_2，t_3）を格納部２２ｂのT_{Ub}にそれぞれ格納する。

ステップ２０５）　制御部２１ｂは、耐タンパ装置２８ｂの制御部２３ｂにセッション情報（s_1，s_2）の生成を依頼する。制御部２３ｂは、以下の手順により（s_1，s_2）を生成し、制御部２１ｂに転送する。

【００８９】

（ａ）　耐タンパ装置２８ｂの番号生成部２６ｂにより番号r_{Ub}の払出しを受

ける。

（ｂ）　r_{Ub}を耐タンパ装置２８ｂの格納部２７ｂの番号集合R_{Ub}に追加する。

（ｃ）　（s_1，s_2）＝（Ｈ（ＰｋＵｂ），r_{Ub}）を生成する。ここで、ＰＫｋＵｂは、制御部２１ｂが保持する検証鍵である。

【００９０】

ステップ２０６）　制御部２１ｂは、利用者装置２の制御部２１ａに（s_1，s_2）を転送する。

ステップ２０７）　利用者装置２ａの制御部２１ａは、耐タンパ装置２８ａの制御部２３ａに（s_1，s_2）と譲渡対象チケットのハッシュＨ（ｍ）を転送する。

【００９１】

ステップ２０８）　利用者装置２ａの耐タンパ装置２８ａの制御部２３ａは、格納部２７ａに格納されたC_{Ua}について、以下の式が成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部２１ａに処理の失敗を通知する。

$$\exists c_1 \ ((H(m), c_2) \in C_{Ua}) \qquad (7)$$

式（７）は、譲渡対象チケットｍに対応するトークン（Ｈ（ｍ）．c_2）が耐タンパ装置２８の格納部２７ａに格納されていることも検証である。

【００９２】

ステップ２０９）　耐タンパ装置２８ａの制御部２３ａは、署名部２５ａが備えるS_{PkUa}と発行者装置１の制御部１１が保持する検証鍵ＰｋＵａ，ＰｋＡａ及び、鍵証明書（ＰｋＵａ，S_{PkAa}（ＰｋＵａ））を用い、トークン交換形式ｅ＝（e_1，e_2，e_3，e_4，e_5，e_6，e_7，e_8）を得る。ここで、ｅの各要素は以下の値をとる。

【００９３】

$e_1 = H(m)$

$e_2 = c_2$

$e_3 = s_1$

$e_4 = s_2$

$e_5 = S_{PkUa}(H(m) \| c_1 \| s_1 \| s_2)$

$e_6 = PkUa$

$e_7 = S_{PkAa}(PkUa)$

$e_8 = PkAa$

ステップ２１０）　利用者装置２ａの耐タンパ装置２８ａの制御装置２３ａは、s_2が正であるなら、C_{Ua}から（H（m），c_2）を削除する。

【００９４】

ステップ２１１）　耐タンパ装置２８ａの制御部２３ａは、制御部２１ａにｅを転送する。

ステップ２１２）　制御部２１ａは、利用者装置２ｂの制御部２１ｂにｅを転送する。

ステップ２１３）　制御部２１ｂは、耐タンパ装置２８ｂの制御部２３ｂにｅ．（t_1，t_2，t_3）を転送し、ｅ内のトークンの格納を依頼する。

【００９５】

ステップ２１４）　制御部２３ｂは、認証部２４ｂを用いて、以下の式の全てが成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部２１ｂに処理の中断を通知する。

$$e_3 = H(PkUb) \quad (8)$$

$$e_4 \in R_{Ub} \quad (9)$$

$$V_{e6}(e_1 \| e_2 \| e_3 \| e_4, e_5) = 1 \quad (10)$$

$$V_{e6}(e_6, e_7) = 1 \quad (11)$$

$$H(e_8) \in t_1 \quad (12)$$

$$V_{t3}(t_1, t_2) = 1 \quad (13)$$

$$e_2 = H(t_3) \quad (14)$$

式（８）及び式（９）は、セッション情報の正当性の検証である。この検証により、当該利用者装置２ｂ以外に宛られたトークン交換形式を格納すること、及びトークン交換形式の再利用によってトークンを複製すること、などによる不正を防止する。

【００９６】

式（１０）は、トークン交換形式に対する署名の正当性の検証であり、この検証によりトークン交換形式の改竄を防止する。

式（１１）は、当該署名者の鍵証明書の検証である。また、式（１２）は、該鍵証明書の署名者が、信任情報中の信任対象に含まれることの検証であり、式（１３）は、該信任情報の正当性の検証であり、式（１４）は、該信任情報の署名者が該トークンの発行者と等しいかどうかの検証である。これらの検証により、該発行者が信用する者によって、該トークン交換形式転送元の耐タンパ性が保証されていることを確認する。

【００９７】

ステップ２１５）　利用者装置２の耐タンパ装置２８ｂの制御部２３ｂは、格納部２７ｂのR_{Ub}からe_4（$=r_{Ub}$）を削除する。

ステップ２１６）　制御部２３ｂは、格納部２７ｂのC_{Ub}に（e_1，e_2）を追加する。

ステップ２１７）　制御部２３ｂは、制御部２１ｂに処理の正常終了を通知する。

【００９８】

ステップ２１８）　制御部２１ｂは、以下の式が成立することを検証する。検証に失敗した場合は処理の中断を、検証に成功した場合は処理の正常終了を、制御部２１ａに通知する。

$$e_1 = H(m) \qquad (15)$$

$$e_2 \in I_{Ub} \qquad (16)$$

式（１５）及び式（１６）は、転送されたトークンが、対象となるチケットに対応し、正当な発行者によって発行されたものであることの検証である。この検証により、譲渡されたチケットが有効であることを確認する。

【００９９】

（３）　チケット消費の場合：

以下は、利用者装置２から改札者装置３に対する接続装置４を介したチケット消費処理の流れである。

図１０は、本発明の一実施例のチケット消費の場合の動作を示すシーケンスチャートである。

【０１００】

なお、同図において、利用者装置２と改札者装置３間に存在する接続装置４は省略する。

ステップ３０１）　利用者装置２の制御部２１は、格納部２２が保持するM_Uから譲渡対象となるチケットｍを抽出する。

ステップ３０２）　制御部２１は、格納部２２が保持するT_Uからｍの発行者による信任情報（t_1，t_2，t_3）を抽出する。

【０１０１】

ステップ３０３）　制御部２１は、改札者装置３の制御部３１にｍと（t_1，t_2，t_3）を転送する。

ステップ３０４）　制御部３１は、以下の手順により（s_1，s_2）を生成する。

（ａ）　番号生成部３３により番号r_Eの払出しを受ける。

【０１０２】

（ｂ）　r_Eを格納部３４の番号集合R_Eに追加する。

（ｃ）　（s_1，s_2）＝（Ｈ（ＰｋＥ），r_E）を生成する。ここで、ＰｋＥは制御部３１が保持する検証鍵である。

ステップ３０５）　制御部３１は、利用者装置２の制御部２１に（s_1，s_2）を転送する。

【０１０３】

ステップ３０６）　制御部２１は、耐タンパ装置２８の制御部２３に（s_1，s_2）と消費対象チケットのハッシュＨ（ｍ）を転送する。

ステップ３０７）　耐タンパ装置２８の制御部２３は、格納部２７に格納されたC_Uについて、以下の式が成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部２１に処理の失敗を通知する。

【０１０４】

$$\exists_{c2}((H(m), c_2) \in C_U \qquad (17)$$

式（１７）は、譲渡対象チケットｍに対応するトークン（Ｈ（ｍ），c_2）が耐タンパ装置２８の格納部２７に格納されていることの検証である。

ステップ３０８）　耐タンパ装置２８の制御部２３は、署名部２５が備えるS_{PkU}と利用者装置２の制御部２１が保持する検証鍵ＰｋＵ，ＰｋＡ及び、鍵証明書（ＰｋＵ，S_{PkA}（ＰｋＵ））を用い、トークン交換形式ｅ＝（e_1，e_2，e_3，e_4，e_5，e_6，e_7，e_8）を得る。ここで、ｅの各要素は以下の値を採る。

【０１０５】

e_1＝Ｈ（ｍ）

e_2＝c_2

e_3＝s_1

e_4＝s_2

e_5＝S_{PkU}（Ｈ（ｍ）‖c_2‖s_1‖s_2）

e_6＝ＰｋＵ

e_7＝S_{PkA}（ＰｋＵ）

e_8＝ＰｋＡ

ステップ３０９）　耐タンパ装置２８の制御部２３は、s_2が正であるなら、C_Uから（Ｈ（ｍ），c_2）を削除する。

【０１０６】

ステップ３１０）　耐タンパ装置２８の制御部２３は、制御部２１にｅを転送する。

ステップ３１１）　制御部２１は、改札者装置３の制御部３１にｅを転送する。

ステップ３１２）　認証部３２を用い、以下の式の全てが成立することを検証する。検証に失敗した場合、以後の処理を中断し、利用者装置２の制御部２１の処理の中断を通知する。

【０１０７】

$$e_3 = H(PkE) \qquad (18)$$

$$e_4 \in R_E \qquad (19)$$

$$V_{e6}(e_1 \| e_2 \| e_3 \| e_4, e_5) = 1 \quad (20)$$

$$V_{e6}(e_6, e_7) = 1 \quad (21)$$

$$H(e_8) \in t_1 \quad (22)$$

$$V_{t3}(t_1, t_2) = 1 \quad (23)$$

$$e_2 = H(t_3) \quad (24)$$

式（１８）及び式（１９）は、セッション情報の正当性の検証である。この検証により、当該改札者装置３以外に宛られたトークン交換形式の利用や、トークン交換形式の再利用などによる不正を防止する。

【０１０８】

式（２０）は、トークン交換形式に対する署名の正当性の検証であり、この検証により、トークン交換形式の改竄を防止する。

式（２１）は、当該署名者の鍵証明書の検証である。また、式（２２）は、該鍵証明書の署名者が、信任情報中の信任対象に含まれることの検証であり、式（２３）は、該信任情報の正当性の検証であり、式（２４）は、該信任情報の署名者が該トークンの発行者と等しいかどうかの検証である。これらの検証により、該発行者が信用する者によって、該トークン交換形式転送元の耐タンパ性が保証されていることを確認する。

【０１０９】

ステップ３１３）　改札者装置３の制御部３１は、格納部３４のR_Eからe_4（$=r_E$）を削除する。

ステップ３１４）　制御部３１は、以下の式が成立することを検証する。検証に失敗した場合は、処理に中断を利用者装置２の制御部２１に通知する。検証に成功した場合は、mに対応するサービスをチケットの消費者に提供する。

【０１１０】

$$e_1 = H(m) \quad (25)$$

$$e_2 \in I_E \quad (26)$$

式（２５）及び式（２６）は、転送されたトークンが対象となるチケットに対応し、正当な発行者によって発行されたものであることの検証である。この検証により、消費されたチケットが有効であることを確認する。

【０１１１】

（４）　チケット提示の場合：

チケット提示は、（３）チケット消費の場合の処理において、以下の変更を加えることにより可能になる。

・ステップ３０４の（ｃ）において、（s_1，s_2）＝（Ｈ（ＰｋＥ），－r_E）を生成する。

【０１１２】

・ステップ３１２において、式（１９）を$-e_4 \in R_E$とする。

以上の変更により、s_2が負数となるため、ステップ３０９において、C_Uからの削除は行われない。即ち、送信側の利用者装置２に有効なチケットを残したまま、当該利用者装置２が該提示時点で有効なチケットを保持していることを検証すること、即ち、チケットの検札が可能となる。

【０１１３】

なお、以上のそれぞれの場合（１）～（４）の説明において、転送されたトークン交換形式は、明示的に保存しなかった。しかしながら、該トークン交換形式の格納部２２などに保存しておき、該トークン交換形式及びｍの受信の際に共に受信したトークン交換形式の履歴をｍの送信の際に共に送信することにより、耐タンパ装置２８が破られるなどして不正行為（二重使用）が発見された場合に、不正が行われた装置を特定することが可能となる。

【０１１４】

また、上記の実施例は、図３～図６に示す構成に基づいて説明したが、この例に限定されることなく、発行者装置、利用者装置、改札者装置、及び接続装置の各機能をプログラムとして構築し、発行者装置、利用者装置、改札者装置、及び接続装置として利用されるコンピュータに接続されるディスク装置や、フロッピーディスク、ＣＤ－ＲＯＭ等の可搬記憶媒体に格納しておき、本発明を実施する際にインストールすることにより、容易に本発明を実現できる。

【０１１５】

なお、本発明は、上記の実施例に限定されることなく、特許請求の範囲内において、種々変更・応用が可能である。

【０１１６】

【発明の効果】

上述のように、本発明によれば、発行者が信用する経路のみを介してトークンを移送し、利用者や改札者が当該発行者を特定することにより、データに対応するトークンについて、該トークン内のトークン発行者情報が示す発行者以外により、該トークンをトークン格納部に新規に格納することを防止すると共に、該トークンが転送の過程において複数のトークン格納部に複製されることを防止する。

【０１１７】

また、トークンを原本情報とし、特定の発行者により発行されたトークンを伴うデータのみを原本とすることにより、当該発行者が原本数を制限することが可能となる。

また、ネットワーク上に存在する情報の識別子（ＵＲＬなど）をデータとして用いることにより、該情報の複製不能かつ譲渡可能なアクセス権を実現することができる。

【０１１８】

また、権利内容を記述したチケットないし、当該チケットの識別子を本発明におけるデータとして用い、有効なトークンを伴うチケットのみを有効なチケットとし、利用者や改札者がそれ以外を無効なチケットとして拒否することにより、チケット自体を耐タンパ装置に格納することなしに、チケットの不正な行使（二重使用や不当な複製など）を防止することが可能となる。

【０１１９】

また、プログラムを本発明におけるデータして用い、特定の発行者により発行されたトークンを該プログラムの実行ライセンスとし、プログラムの実行器は、該トークンを伴うプログラム以外の実行を拒否することにより、不当に複製された該プログラムの実行を防止することが可能となる。

また、音楽データや画像データを本発明におけるデータとして用い、特定の発行者により発行されたトークンを該データの鑑賞権として用い、データの表示器もしくは、再生器は該トークンを伴うデータ以外の表示や再生を拒否することに

より、不当に複製された該データの鑑賞を防止することができる。

【図面の簡単な説明】

【図１】

本発明の原理構成図である。

【図２】

本発明の原本流通システムにおけるデータ蓄積システムの構成図である。

【図３】

本発明の一実施例の発行者装置の構成図である。

【図４】

本発明の一実施例の利用者装置の構成図である。

【図５】

本発明の一実施例の改札者装置の構成図である。

【図６】

本発明の一実施例の接続装置の構成図である。

【図７】

本発明の一実施例のチケット発行の場合の動作を示すシーケンスチャートである。

【図８】

本発明の一実施例のチケット譲渡の場合の動作を示すシーケンスチャート（その１）である。

【図９】

本発明の一実施例のチケット譲渡の場合の動作を示すシーケンスチャート（その２）である。

【図１０】

本発明の一実施例のチケット消費の場合の動作を示すシーケンスチャートである。

【符号の説明】

１　発行者装置

２　利用者装置

３　改札者装置

４　接続装置

１１　制御部

１２　署名部

１３　データ生成部

１４　トークン生成部

１５　信任情報生成部

２１　制御部

２２　格納部

２３　制御部

２４　認証部

２５　署名部

２６　番号生成部

２７　格納部

２８　耐タンパ装置

３１　制御部

３２　認証部

３３　番号生成部

３４　格納部

４１　通信部

１００　発行者装置

１１０　第１の原本性情報生成手段

１２０　第１の原本性情報転送手段

２００　利用者装置

２１０　第２の原本性情報転送手段

２２０　第１の特定手段

２３０　第１の認証手段

２４０　格納手段

３００　改札者装置

３１０　第２の特定手段

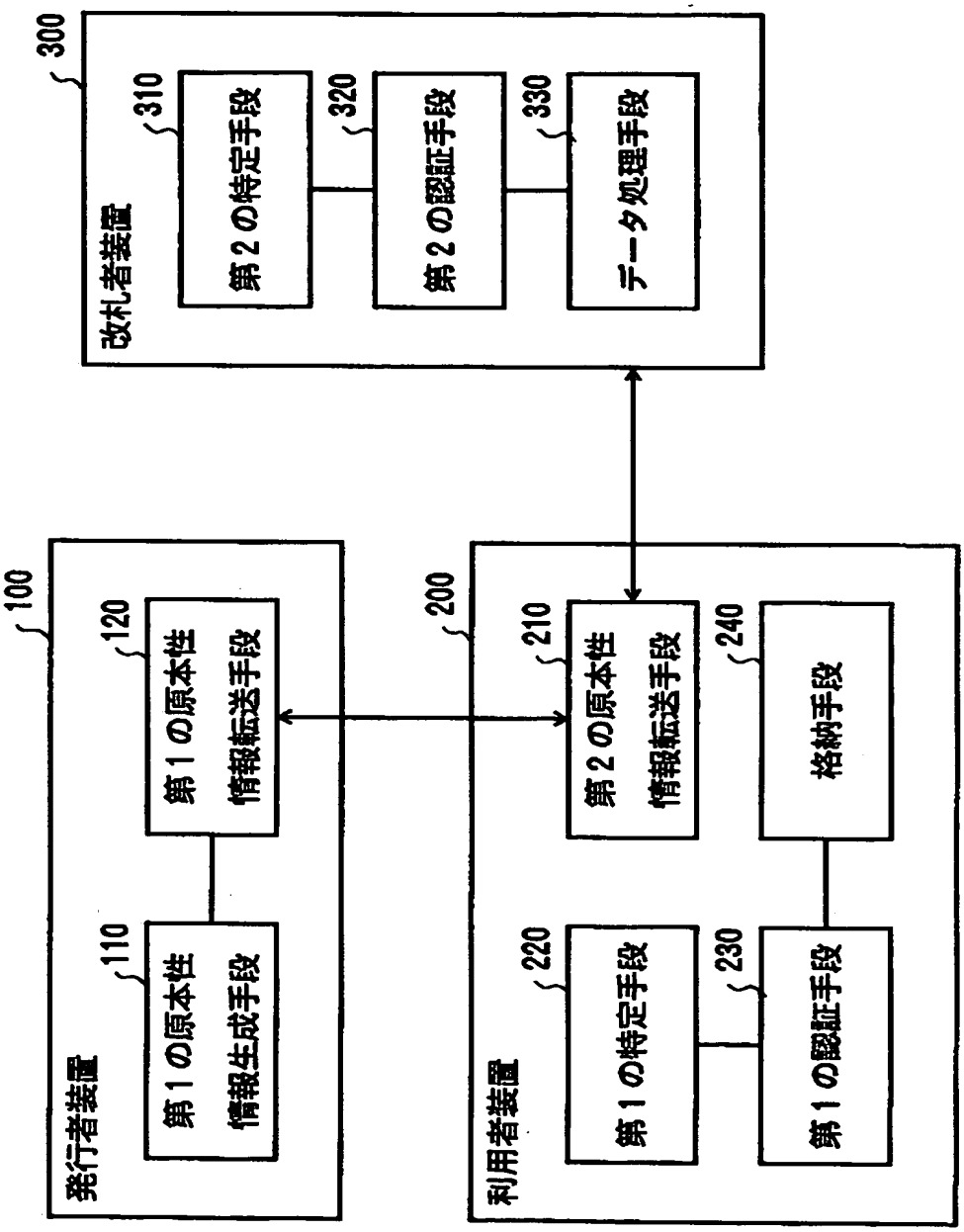
３２０　第２の認証手段

３３０　データ処理手段

【書類名】　図面

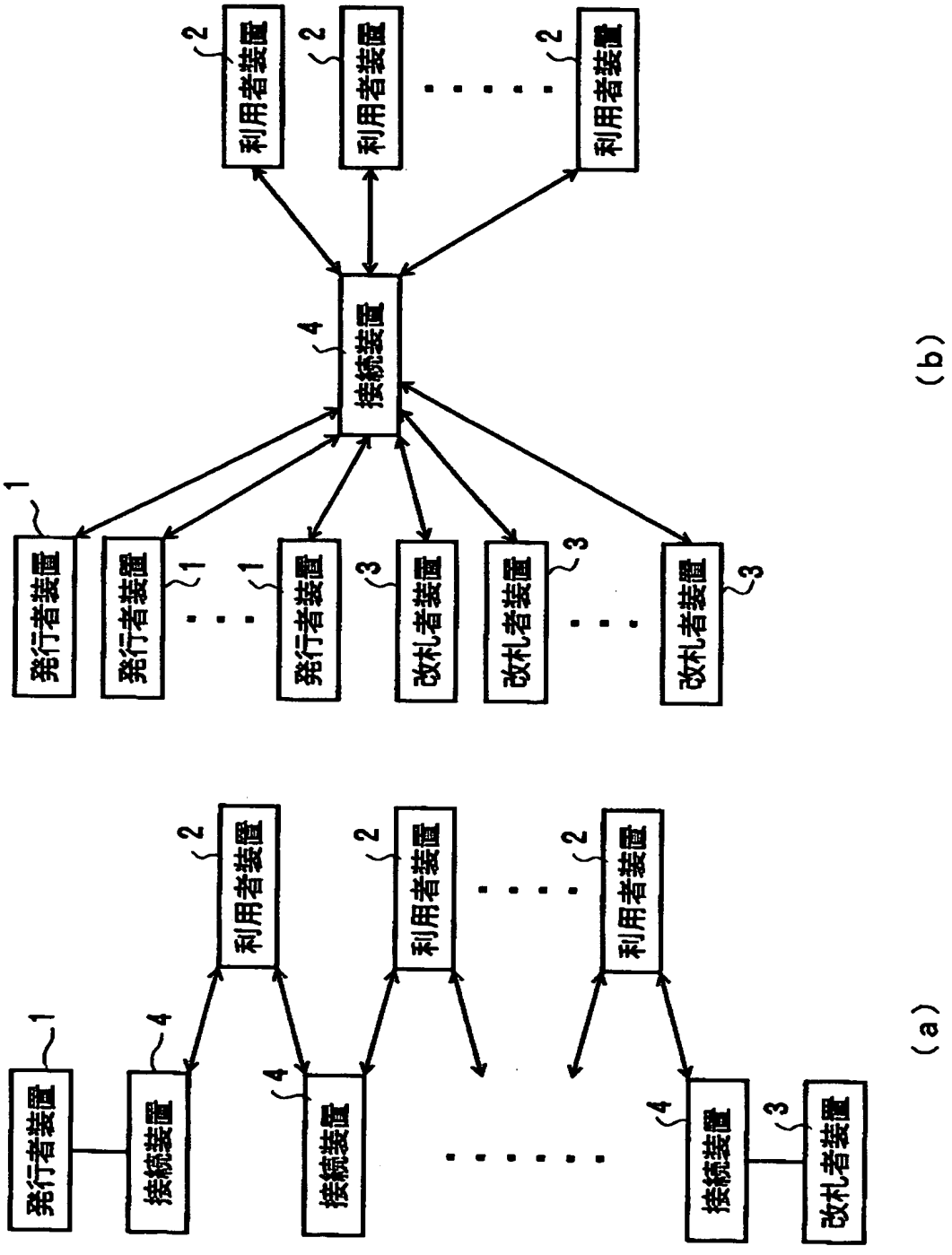
【図１】

本発明の原理構成図



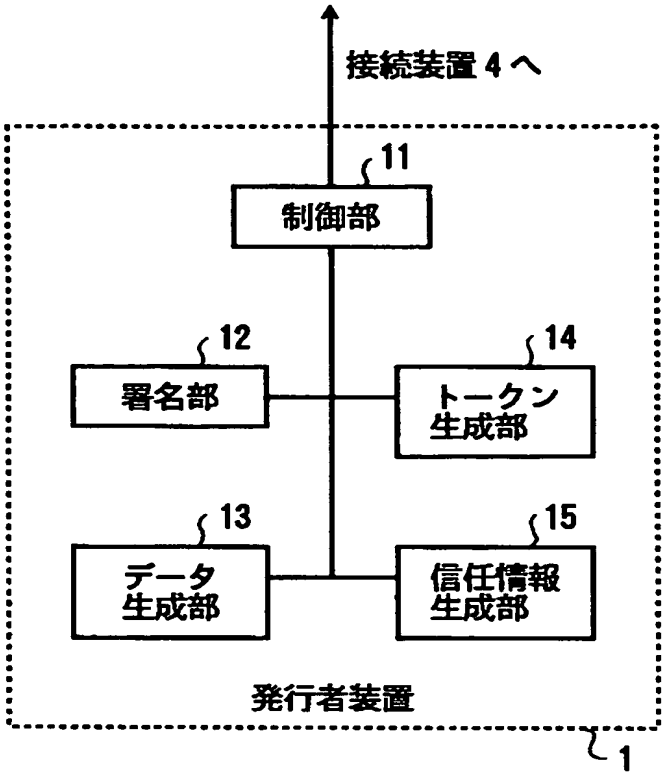
【図２】

本発明の原本流通システムにおけるデータ蓄積システムの構成図



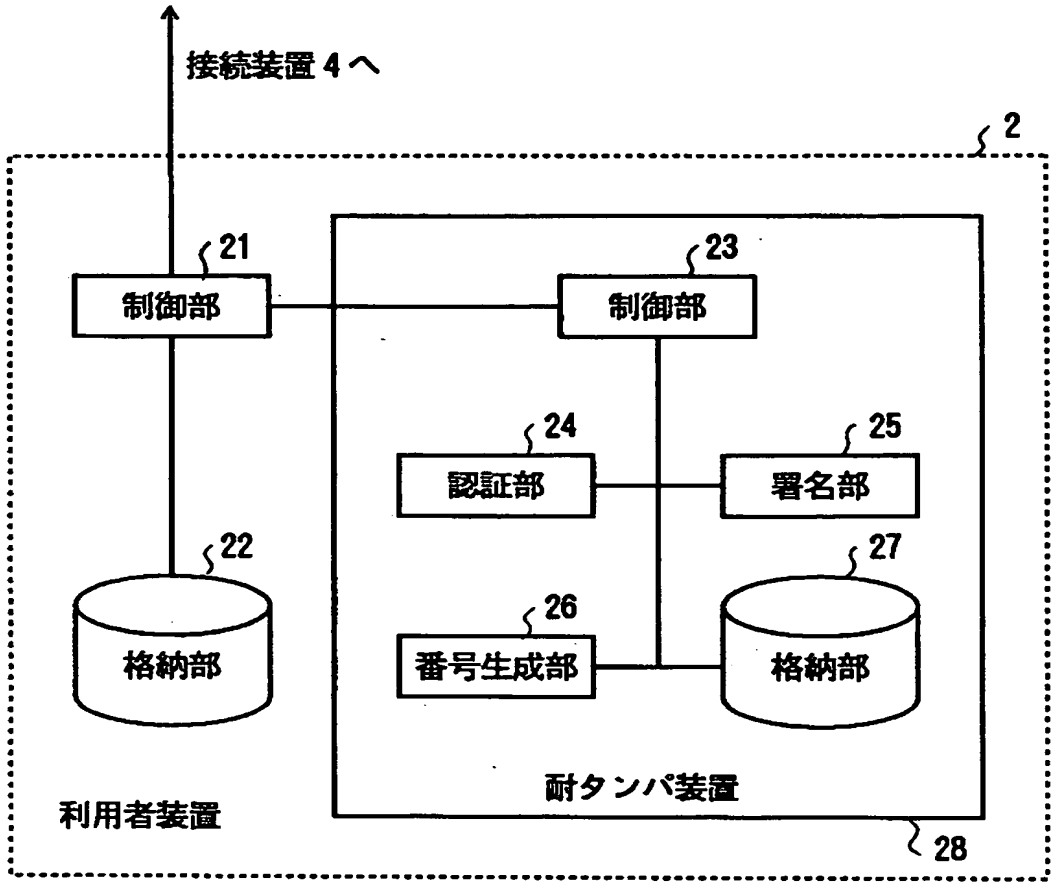
【図３】

本発明の一実施例の発行者装置の構成図



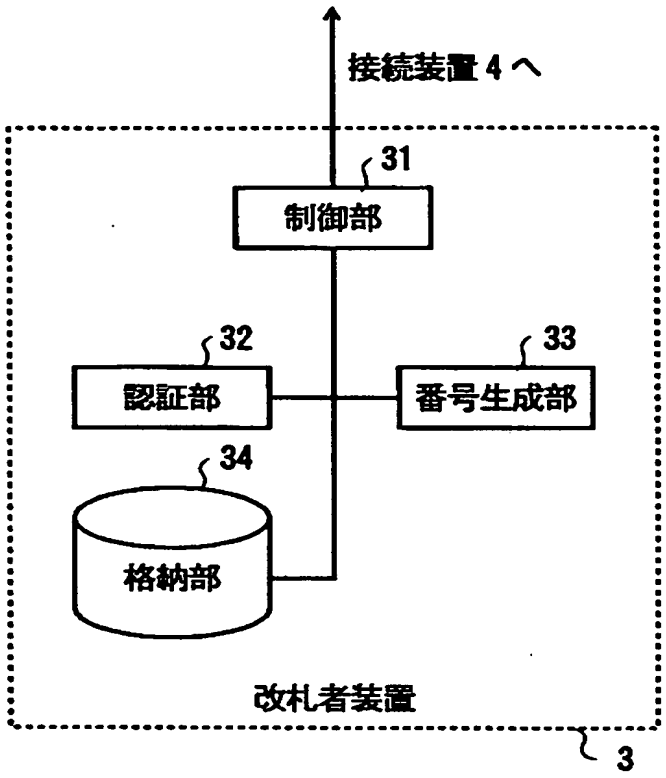
【図４】

本発明の一実施例の利用者装置の構成図



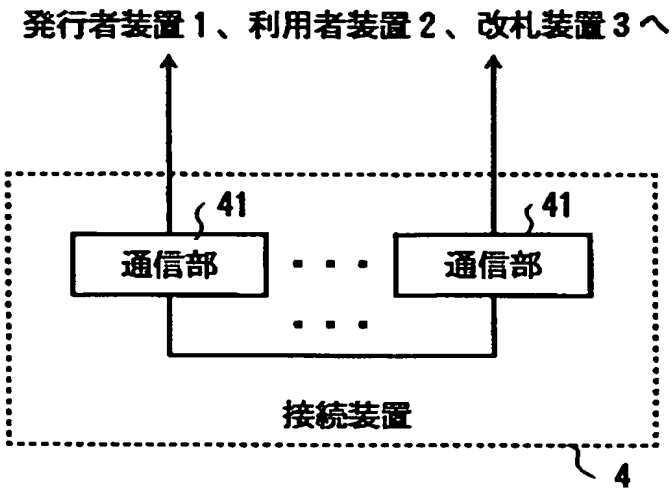
【図５】

本発明の一実施例の改札者装置の構成図



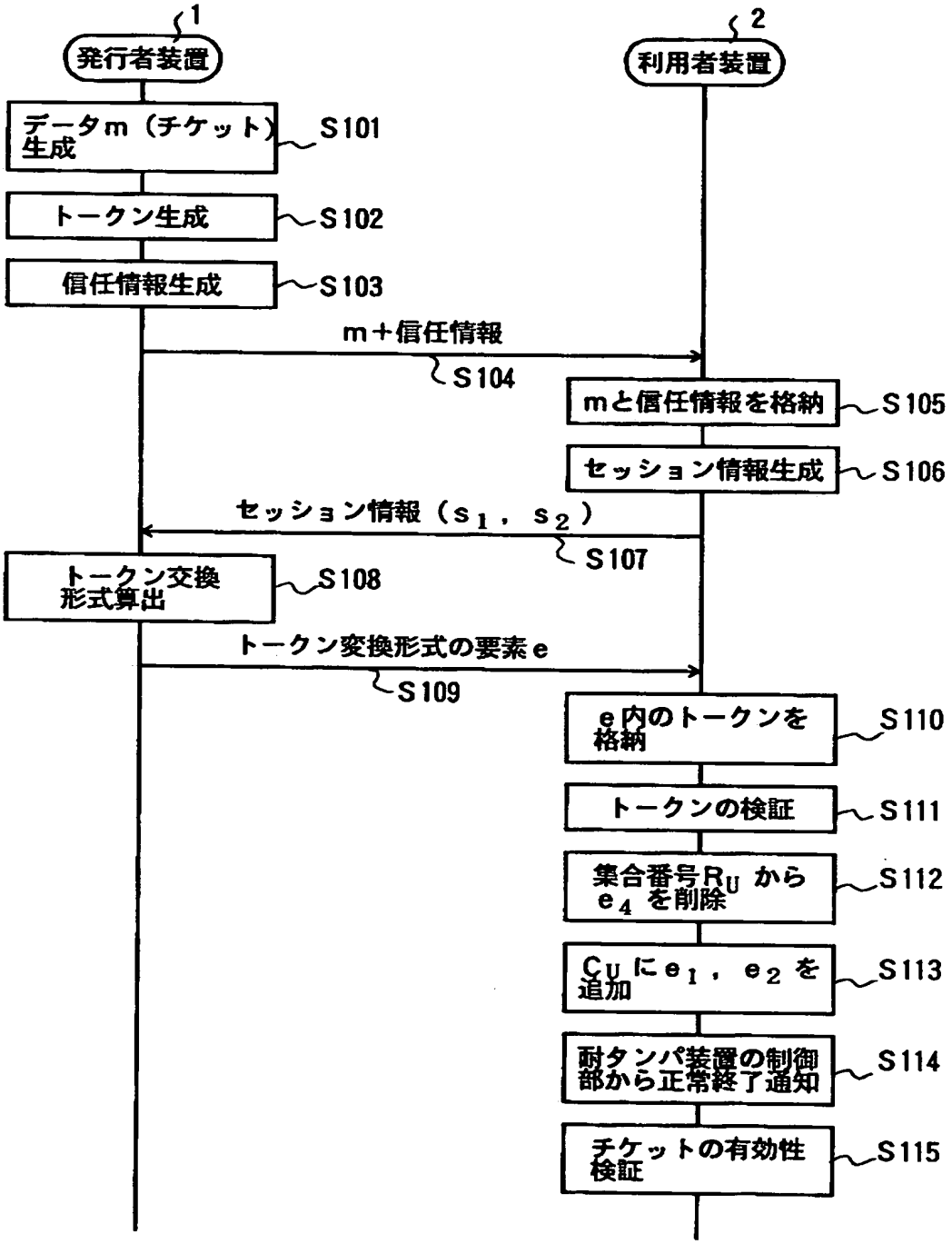
【図６】

本発明の一実施例の接続装置の構成図



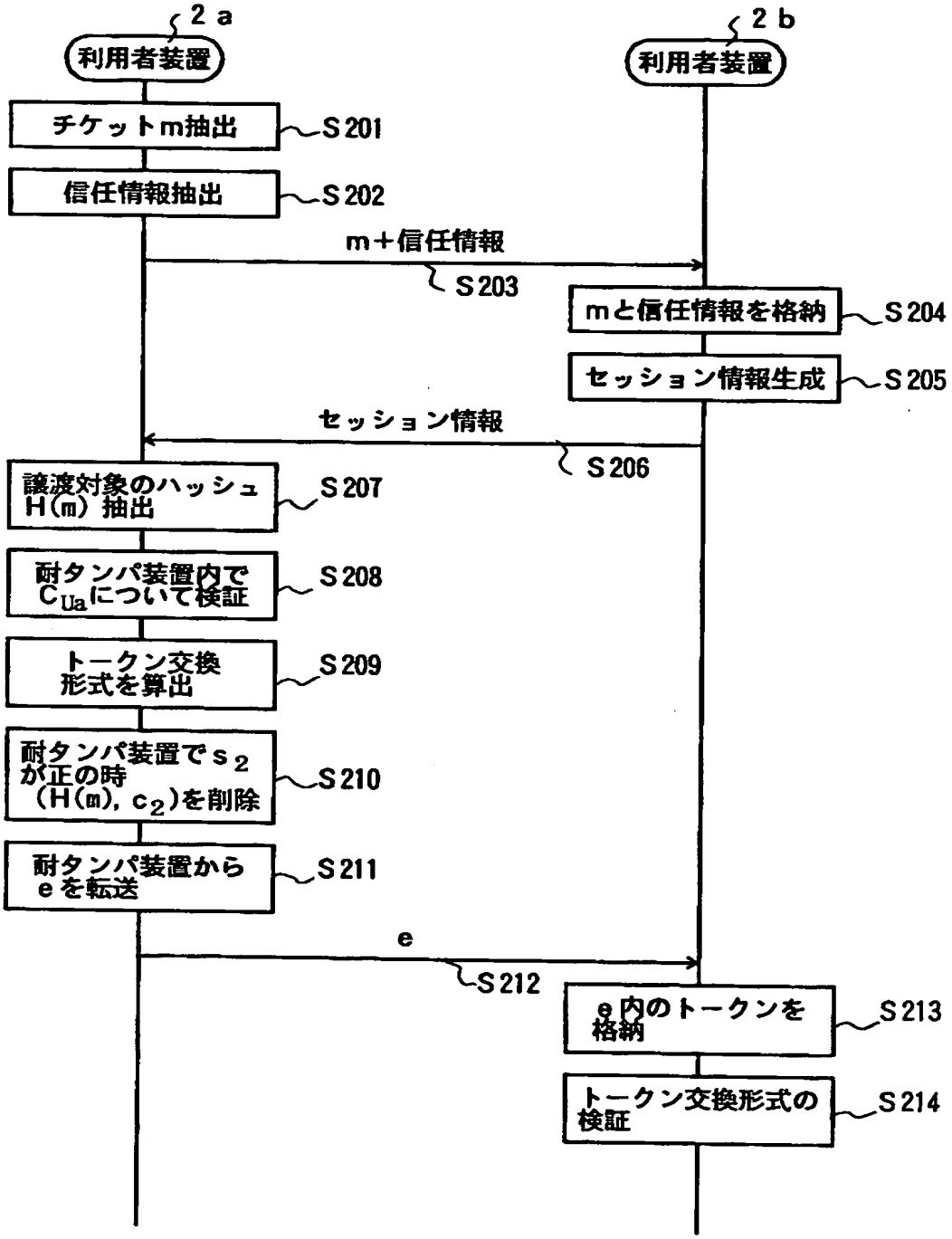
【図７】

本発明の一実施例のチケット発行の場合の動作を示すシーケンスチャート



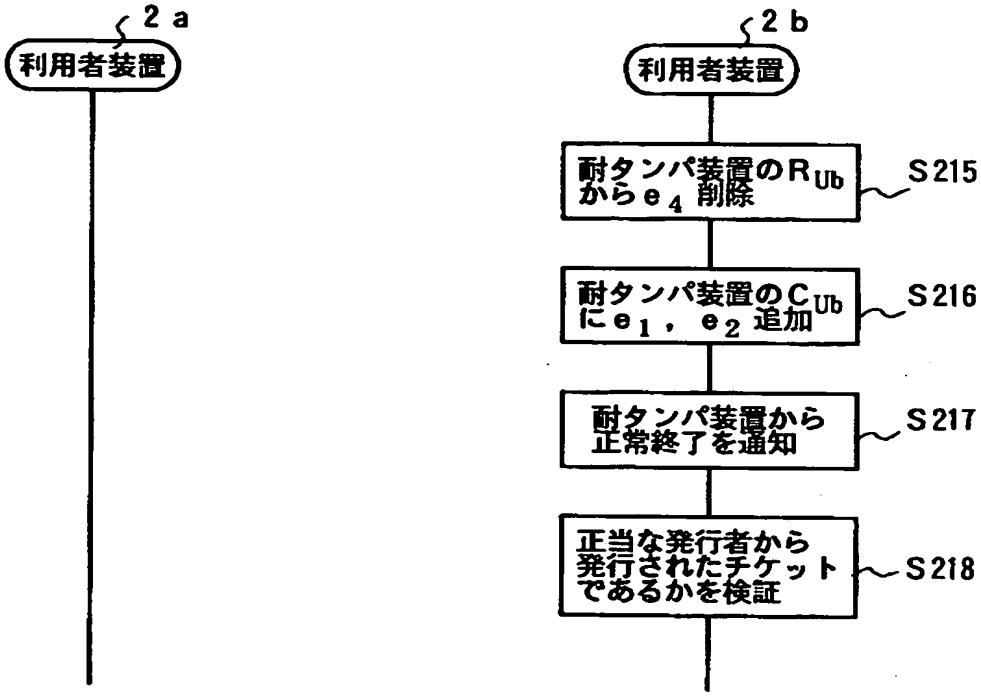
【図８】

本発明の一実施例のチケット譲渡の場合の動作を示すシーケンスチャート（その１）



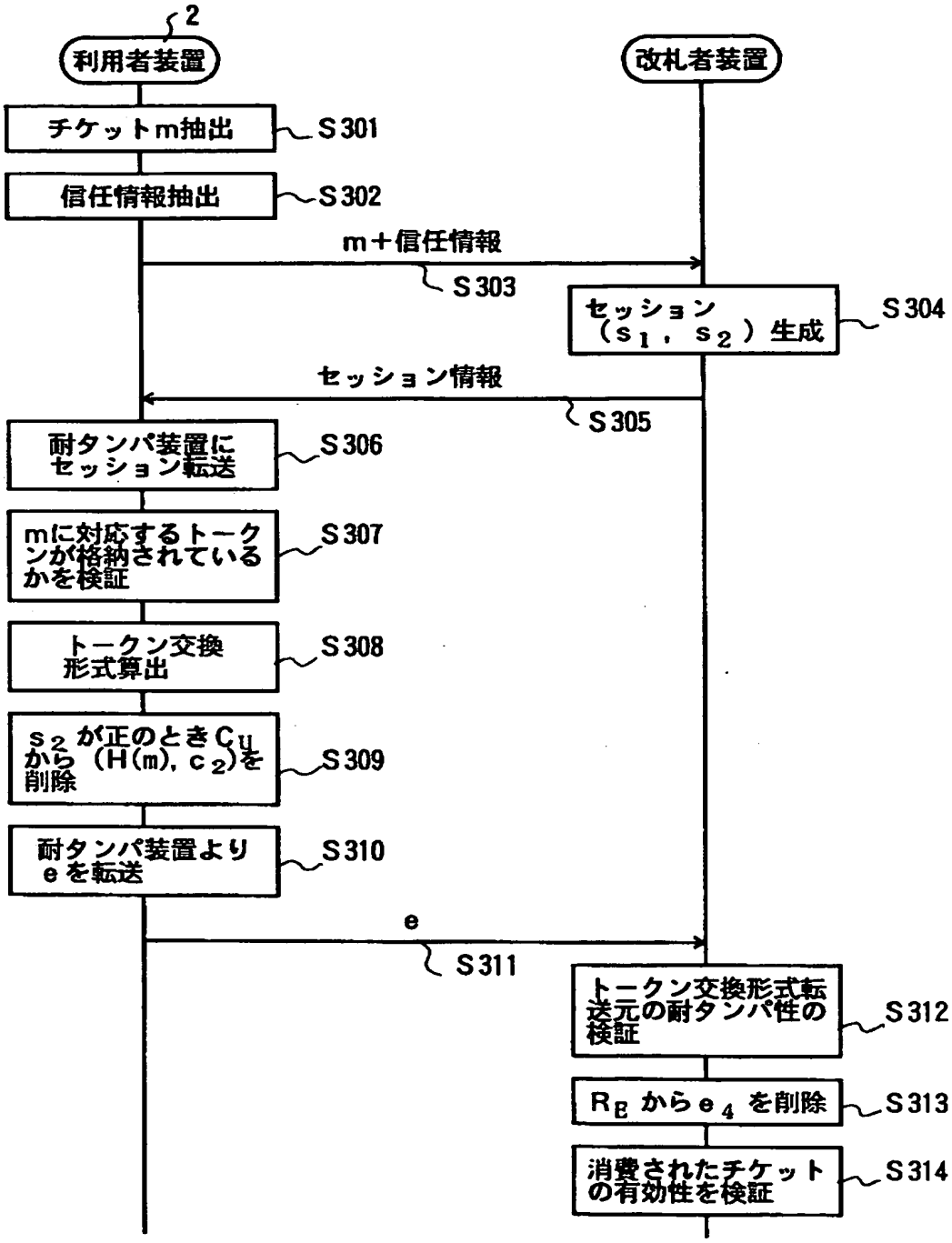
【図９】

本発明の一実施例のチケット譲渡の場合の動作を示すシーケンスチャート（その２）



【図１０】

本発明の一実施例のチケット消費の場合の動作を示すシーケンスチャート



【書類名】　　要約書

【要約】

【課題】　トークンの生成やデータの流通などにおける負荷を低減する原本データ流通システム及び原本データ流通プログラムを格納した記憶媒体を提供する。

【解決手段】　本発明は、ある装置に対応する第１の情報と、データもしくは、データに対応する情報である第２の情報と、から構成される原本性情報を転送する転送手段を有する第１の装置と、原本性情報の転送元装置を特定する特定手段と、該転送元装置が認証された場合、もしくは、該転送元装置と該原本性情報の第１の情報に対応する装置とが同一であった場合のみ、該原本性情報を有効であると判別する認証手段とを有する第２の装置とを有する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００４２２６〕

１．変更年月日　　１９９９年　７月１５日
［変更理由］　住所変更
住　所　東京都千代田区大手町二丁目３番１号
氏　名　日本電信電話株式会社